

Cyber Security

الأمن السيبراني

المفهوم وتحديات العصر

الدكتور فارس محمد العمارات

عميد متقاعد إبراهيم الحمامة





الأمن السيبراني
المفهوم وتحديات العصر

الأمن السيبراني

المفهوم وتحديات العصر

جميع الحقوق محفوظة للناشر © لا يسمح بإعادة إصدار هذا الكتاب أو أي جزء منه أو تخزينه أو استنساخه أو نقله، كليا أو جزئيا، في أي شكل وبأي وسيلة، سواء بطريقة إلكترونية أو آلية، بما في ذلك الاستنساخ التكنولوجي، أو التسجيل أو استخدام أي نظام من نظم تخزين المعلومات واسترجاعها، بدون الحصول على إذن خطي مسبق بالواقعة من الناشر.

Copyright © All rights reserved to the publisher. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without prior permission in writing of the publisher.

الطبعة الأولى

2022

(الآراء الواردة في الكتاب لا تعبر بالضرورة عن رأي الناشر)

دار الخليج للنشر والتوزيع

الأردن: عمان، العبدلي تلفاكس: 00962 6 464 7559

daralkhalij@gmail.com daralkhalij1998 daralkhalij



الأمن السيبراني

المفهوم وتحديات العصر

الدكتور

فارس محمد العمارات

العميد المتقاعد

إبراهيم محمد الحمامصه



رقم الإيداع لدى دائرة المكتبة الوطنية

(2022/6/ 2820)

005.8

العمارات، فارس محمد

الأمن السيبراني: المفهوم وتحديات العصر / فارس محمد

العملات / إبراهيم محمد الحمامصة، 2022

الواصفات: / أمن البيانات // الجرائم الحاسوبية// حماية

البيانات//الأمن القومي//شبكات المعلومات/

- يتحمل المؤلف كامل المسؤولية القانونية عن محتوى

مصنفه ولا يعبر عن رأي دائرة المكتبة الوطنية أو أي جهة

حكومية أخرى.

ISBN: 978-9923-23-129 -6

الإهداء

إلى الذين يعملون خلف الكواليس يقاتلون الأعداء المُفترضين
إلى الجنود الذين ينافحون عن الوطن ليبقى سليماً من الأذى الرقمي
سلاماً وتحية»

المحتويات

9.....	مقدمة
11.....	الفصل الأول: ماهية الأمن السيبراني
13.....	المبحث الأول : مفهوم الأمن السيبراني
25.....	المبحث الثاني: الأمن السيبراني الأهمية والأبعاد
41.....	الفصل الثاني: التهديدات والجريمة السيبرانية
43.....	المبحث الأول: التهديدات السيبرانية
51.....	آليات مواجهة التهديدات السيبرانية
71.....	المبحث الثاني: الجريمة السيبرانية
91.....	الفصل الثالث: الإرهاب والهجمات السيبرانية
91.....	المبحث الأول: الإرهاب السيبراني
103.....	المبحث الثاني: الهجمات السيبرانية
121.....	الفصل الرابع: الحروب السيبرانية
133.....	المبحث الثاني: تداعيات الحروب السيبرانية على الأمن القومي:
143.....	الفصل الخامس: الجهود الدولية، والتنظيم الدولي
143.....	مكافحة الهجمات السيبرانية
145.....	المبحث الأول: الجهود الدولية في مجال مكافحة الإرهاب السيبراني
149.....	المبحث الثاني: التنظيم الدولي لمكافحة الهجمات السيبرانية
174.....	المبحث الثالث: ادارة الخطر السيبراني
183.....	الفصل السادس: السيبرانية ساحة الحرب القادمة
183.....	المبحث الأول: ماهية ساحة الحرب القادمة
192.....	المخاطر والتداعيات:

195.....	المبحث الثاني: مستقبل الحروب السيبرانية
205.....	الخاتمة
207.....	المراجع والمصادر



مقدمة

لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات اللامتناهية أو اللاتناظرية العابرة للحدود التي لا تعترف بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية.

ومع إنفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن 21 وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني "cyber security" كبُعد جديد ضمن أجندة حقل الدراسات الأمنية وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

وأصبح الأمن السيبراني مطلباً ضرورياً لكل الدول دون إستثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والإختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى

وشبكة الإنترنت بشكل عام، ويعمل مختصو الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات.

فالمارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية والهامة أو يعدلون ويحرفون في معلومات مهمة أو حتى يثبتوا معلومات غير صحيحة على مواقع مهمة، وذلك عندما يكون الأمن السيبراني ضعيفاً ويحتاج لتقوية بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية، وأمن المعلومات ليس بعيداً عن الأمن السيبراني، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة والاختراق، ويمنع أي شخص غير مصرح له بالوصول إليها من ذلك، ومن هنا ولأهمية هذا الجانب في حياة الدولة وحياة الأفراد جاءت هذه الدراسة ليستفيد منها الجميع



الفصل الأول

ماهية الأمن السيبراني

لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات اللامثالية أو اللاتناظرية العابرة للحدود التي لا تعترف بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية.

لقد أصبح الأمن السيبراني مطلباً ضرورياً لكل الدول دون استثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكل عام، ويعمل مختصو الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات، فالمارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية والهامة أو يعدلون ويحرفون في معلومات مهمة أو حتى ييشوا معلومات غير صحيحة على مواقع مهمة، وذلك عندما يكون الأمن السيبراني ضعيفاً ويحتاج لتقوية، بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية، وأمن المعلومات ليس بعيداً عن الأمن السيبراني، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه

وليس حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة والاختراق،
ويمنع أي شخص غير مصرح له بالوصول إليها من ذلك، ولأهمية هذه الحماية
قامت الوطن باستطلاع مدى الوعي المجتمعي بأهمية الأمن السيبراني وأمن
المعلومات من خلال إجراء آراء عدد من المهتمين.

المبحث الأول : مفهوم الأمن السيرياني

تُعتبر مهمة ضبط المفاهيم والمصطلحات تحدياً يواجهه مختلف الباحثين والدارسين في مختلف التخصصات، وذلك لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين أعضاء المجتمع العلمي، ويعد الأمن السيرياني واحداً من المفاهيم المعقدة التي قدمت لها العديد من التعريف المختلفة .

والأمن السيرياني لغوياً : مكوّن من لفظتين: "الأمن"، و"السيرياني"

الأمن: هو نقيض الخوف، أي بمعنى السلام، والأمن مصدر الفعل أَمِنَ أَمْنًا وَأَمَانًا وَأَمْنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه، وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة .

وعلى الرغم من أن مصطلح الأمن القومي قد شاع بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وبخاصة بعد معاهدة وستفاليا عام 1648 التي أسست لولادة الدولة القومية أو الدولة **Nation** والامة **State** ، وشكلت حقبة الحرب الباردة الإطار والمناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية وأطر مؤسساتية وصولاً إلى إستخدام تعبير "إستراتيجية الأمن القومي"، وسادت مصطلحات الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.(بلقزيز،1989)

وقد تبنى آخرون مصطلح الحرب السيبرانية "Cyber Warfare" بالاستناد إلى أيدولوجية أمنية أو عسكرية تضع منهاجاً لتحقيق الأهداف على الصعيد الأمني أو العسكري، تجاه "العدو المفترض". (غانم، 1962)

أما البعض الآخر فاختار مصطلح الهجمات السيبرانية "Attacks Cyber" كوصف واقعي يجمع بين فهو تصرف يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصال كل ما ذكر آنفاً تعمل إلكترونياً، ومن ثم تطور ليتضمن مفهوماً أوسع، يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق مواقع الكترونية حساسة، عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات، ووسائل النقل الأخرى. (الفتلاوي، 2016)

ولأن مصطلح الحرب هو مصطلح غير مُحبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي فيكون مصطلح الهجمات السيبرانية أكثر قرباً للموضوع الذي تتناوله هذه الدراسة، ولا سيما أن تصرفات دولية عدة أشارت إلى مصطلح الهجمات، وعدتها بمثابة التصرف الذي يوضع في الحسبان في أثناء النزاعات المسلحة، طبقاً للقانون الدولي الإنساني. (الفتلاوي، 2016)

والسيبراني: هي مصطلح السيبرانية الآن، وهو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي وتُشير المقاربة الإيتمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مُشتقة من كلمة "Kubernetes" بمعنى الشخص الذي يُدير دفة السفينة، حيث تستخدم مجازاً للمُتحكم "governor" وتُجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات

الأمريكي "Norbert wieners 1894-1964" وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنتيقية من خلال مؤلفه الشهير:

Cybernetics or control and communication in" the Animal and the machine

وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان، والآلة ليستبدل مُصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب. (بوغرة، 2018)

أما إصطلاحياً : هناك العديد من التعريفات التي قُدمت لمفهوم الأمن السيبراني، حيث يُعرّف بأنه: "مجموعة من الإجراءات المُتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المُضادة المطلوبة".

وما ذهب إليه الكاتبان "Pekka, & Martti" في كتابهما الموسوم "Cyber Security: Analytics, Technology and Automation"، حيث اعتبر أن الأمن السيبراني : "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المُضادة المطلوبة". بينما عرّفه إدوارد أمورسو "Amoroso" بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة".

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عُرّف الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن

استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين".
(بوغرة، 2018)

وقدمت وزارة الدفاع الأمريكية "البتاغون" تعريفاً دقيقاً لمصطلح الأمن السيبراني، فاعتبرته: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث".

ويمكن تعريف الأمن السيبراني، أيضاً بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأسوأ الأحوال، ويرتبط هذا الأمن، ارتباطاً وثيقاً، بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف غالب الأحيان، وراء عمليات الاعتداء على الشبكات وعلى الإنترنت بشكل أكثر. (الفتلاوي، 2016)

ومن هنا فإن على الأنظمة الإلكترونية الاعتماد على المعلومة، حقيقة لا لبس فيها، والتي تفرض اعتماداً على التي تُعالجها والحديث عن الأمن، ويستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم إجراءات المفروض اتخاذها، لدفع الخطر، فالتهديد هو نوع الأعمال العدائية، التي يمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الإنكشاف على هذا التهديد، في سياق معين، والإجراءات

التي يفترض اتخاذها، ولا يمكن أن تقتصر في أي حال من الأحوال على التقنية، بل أنها تتناول بناء القدرات، والتوعية، والتدريب، ونقل الخبرات. (بوغراة، 2018)

وعدا عن مجموعة من القواعد المحددة والواضحة، التي يفترض إتباعها، فالخطر يتناول أمن الشبكات وأمن الإنترنت، لناحيتين: (الفتلاوي، 2016)

الأولى: هي البنية التحتية، وما عليها من نقاط دخول وخروج وتخزين، واعتراض للمعلومات.

الثانية: عمليات التخريب والتدمير والتعطيل، التي تطاولها، وتطاول الأموال، والأشخاص من خلالها ولان للشبكة العالمية للمعلومات، مواصفات تقنية وفنية خاصة، تؤسس لمخاطر معينة، فإن اتصال الشبكات بها يعرض هذه الأخيرة للمخاطر التي يتعرض لها النظام، وبذلك، يمكن تصور الإعتداء، يجعله يتوقف عن تأدية الخدمات التي كان يقدمها، أو يجعله يعرض أسرار المؤسسات والأفراد سواء منها الشخصية أو الصناعية والمهنية، أو بما يؤدي إلى تلف البيانات الحساسة، أو بث معلومات مغلوبة.

ولا بد من الإشارة إلى ضرورة التمييز، بين المعلومات وبين التكنولوجيا وأدواتها، فالمعلومة: هي ما ينتج عن معالج البيانات والمعطيات بشكل معين، تستخدم فيه التكنولوجيا، سواء للتجميع، أو للوصول أو للتخزين والمعالجة، لذا فإن أولى خطوات تحقيق الأمن، هي مراقبة هذه التكنولوجيا، لا سيما في شقتها الذي يمثل الإتصالات، ومراقبة حركة انتقال المعلومات، بما يضمن إزالة العوائق أمام الوصول إليها وانسيابها ومنع التنصت، سواء من جانب الطرف المنافس، أو من قبل الطرف الذي يسعى إلى الاعتداء. (بوغراة، 2018)

ومن هنا ضرورة سعي المؤسسات، كما الأفراد، إلى تحقيق أمن الاتصالات، عبر الحفاظ على سريتها مع ما يمكن أن يطرحه هذا الأمر من إشكاليات، تتعلق بمكافحة الجرائم، والحفاظ على الأمن. وبهذا المعنى يكون الأمن، هو عدم السماح باستخدام النظام، الا فيما هو معد لاجله، وفي الاطار المسموح به.

فالأمن السيبراني، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الأصلاح في الاتصالات للعام 2010-2011"، هو مجموعة من اجراءات المهمات، مثل تجميع وسائل، وسياسات، أمنية، ومبادئ توجيهية، ومقاربات ادارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين. (الاتحاد الدولي للاتصالات، 2011)

والدليل على ذلك، هو التنسيق المتزايد بين إدارات الأمن والإقتصاد، إضافة إلى الترابط الذي يراه قادة العالم، بين أمن الأمن السيبراني، والإقتصاد والأمن القومي، ويلامس الأمن السيبراني الأمن القومي بشكل وثيق جداً، فالتقنيات التي وسعت الافاق، وأثرت الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، وباتت تهدد الهوية الوطنية والقومية، مع تأثر الأجيال الصاعدة بما يصلها وبما تصل إليه عبر الإنترنت، حيث تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل، من خلال تكنولوجيا المعلومات، وحرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص، وبيئتهم المميزة، لامن السيبراني كأى مجال آخر، فضاء سيبراني يستحضر الناس فيه قيمهم ومصالحهم، واهتماماتهم المختلفة، التي يمكن أن تتأثر وتؤثر. وبتنا نلاحظ، على سبيل المثال، أن بعض

مجموعات المصالح الخاصة، تهدد بالحلول كبديل لهوية يندمج تحت مظلتها، مجموعات أكبر من الناس. (الفتلاوي، 2016)

وكان من بدهيات، المسؤول السابق عن الأمن الوطني الأمريكي، قد اعتبر، أن الإنترنت قد رفعت مستوى الاخطار التي يتعرض لها النظام بشكل غير مسبوق، وذلك، في إشارة واضحة، القومي، والتي يمكن أن تتخذ اشكالا إلى التهديدات الجديدة، التي تستهدف الأمن غير متوقعة، وتطاول مجالات أساسية وحيوية. كذلك، أعلن الرئيس الأمريكي أوباما، أن أمن السيب ارني، يأتي في مقدمة اهتماماته، معتبراً الأمن السيراني، من أخطر التهديدات التي من المسائل، التي تطرح على المستوى الاقتصادي، كما على مستوى الأمن القومي، وقد ترجم هذا عملياً بتعيين مسؤول عن أمن الأمن السيراني، يكون على اتصال وتنسيق دائمين معه، ويكون عضواً من القومي، وفي المجلس الإقتصادي الوطن، في حين اعتبر الإعلان الأوروبي الأمن السيراني أنه يعني "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".

وهنا تجدر الإشارة إلى أن الأمن السيراني مفهوم أوسع من أمن المعلومات، فالأمن السيراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية"، بينما لا يهتم الأمن السيراني بذلك.

أما إجرائياً: يمكن القول إن الأمن السيراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر "الفضاء السيراني بصفة عامة" من مختلف الهجمات والاختراقات والتهديدات السيرانية التي قد تُهدد الأمن القومي للدول.

ظهور الأمن السيبراني

تكمُن أهمية الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية، ومن خلال مفهوم حرب الإنترنت "netwar" والحرب السيبرانية "cyber war" وقد كان هناك تاريخ واسع من الاختبارات النظرية والأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني. (الفتلاوي، 2016)

ومع نهاية الحرب الباردة، حدثت تحولات تدريجية، ظهرت على مستوى التفكير في الدراسات الأمنية لأن النظرة الضيقة المتمركزة حول الدولة كانت ستاتيكية ثابتة ودائماً ما تؤدي إلى انتقادات حول كيف كان الأمن دائماً مفهوماً تقليدياً.

وضمن مجال الدراسات الأمنية النقدية، يمكن فهم دور الأمن السيبراني وهو ما تجلّى في أعمال مدرسة كوبنهاغن وروادها أمثال: باري بوزان "Barry Buzan" وأولي وييفر "Ole Waever"، حيث اكتسبت أعمالهم أهمية كبرى خاصة عند التفكير في الأمن السيبراني؛ لأن تركيزهم لم يَقم على محاولة موضوعية لتصنيف ما هو التهديد أو ما هي الثغرة الأمنية، بل ما هي الشروط أو الحالة الراهنة التي يجب أن تباشرها جهات فاعلة محددة من أجل إظهار فعل ما بأنه تهديد وهو ما يعرف بعملية الأمانة "the process of securitization"، وهي الإجراء الذي يحدد من خلاله المنظرين ما ينبغي وما لا ينبغي تعريفه بأنه مشكلة أمنية، أي إضفاء الطابع الأمني على قضية معينة.

المفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

الفضاء السيبراني: وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام "ANSSI"، بأنه: "فضاء التواصل المُشكّل من خلال الربط البيئي العالمي لمعدات المُعالجة الآلية للمعطيات الرقمية"، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مُشغلين أو مُستعملين، كما أن هناك مَنْ عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيش الحديثة. (Olivier, 2012)

الردع السيبراني: يُعرف الردع السيبراني بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"، ويرتكز الردع السيبراني على ثلاث ركائز هي عماد استراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع **Credible Defense**، والقدرة على الانتقام "An Ability to Retaliate"، والرغبة في الانتقام "A Will to Retaliate".

الهجمات السيبرانية: يُمكن تعريفها بكونها "فعلاً يقوِّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكن المهاجم من التلاعب بالنظام".

وتعرف الهجمات السيبرانية على أنها فعل يقوِّض من قدرات ووظائف الشبكة المعلوماتية من خلال استغلال أحد نقاط الضعف ما يمنح المهاجم القدرة على التلاعب بالنظام، أما جونيدو مارشال "Marshall junaidu" فيعرفه على أنه عملية الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة، وتتعدد ما بين الأساليب المُمكنة أو العشوائية، فقد تستخدم من طرف الرسميين، أو أساليب ضغط أو بشكل عشوائي من طرف حترفين

لتحقيق النفع الذاتي او المصالح الشخصية او هجمات منظمة من طرف جماعات مارقة. (بونيف،2019).

الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات، أو أجهزة إلكترونية أو شبكة الإنترنت، أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، فهي الجريمة المتصلة باستخدام الكمبيوتر، أو أي تصرف غير قانوني يرتكب باستخدام تقنيات المعلومات والاتصالات.

القوة السيبرانية : يُعد جوزيف ناي "Joseph nay" من أبرز المهتمين بالقوة السيبرانية حيث يعرفها بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات سيبرانية".

ومن الأمور المتعارفة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية "Cyber power" التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين ما جعل قدرة الدولة على السيطرة موضع شك ومن ناحية أخرى منحت الفاعلين الأصغر قدرةً أكبر على ممارسة

كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيرياني، وهو ما يعني تغيرات في علاقات القوى في السياسة الدولية. (Olivier, 2012)

ومن هذا المنطلق أصبح الباحثون في حقل العلاقات الدولية وبقية الحقول الفرعية في الدراسات الأمنية والدراسات الاستراتيجية يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي، ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة والسيادة، الحوكمة العالمية "global governance" وقد وصف (segel, 2016) كيف يعمل توسع الإنترنت على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية التي تعمل على نطاق واسع للدخول في عصر جديد للجيوبوليتيك، وتاريخ هذا التطور هو محور ملف استراتيجي قام بتجميعه المعهد الدولي للدراسات الاستراتيجية بلندن، والذي يعرض بالتفصيل التطور التكنولوجي وآثاره السياسية بدءاً من الخمسينات.

أما على مستوى الجانب الممارساتي للدول، فقد ارتبط ظهور الأمن السيرياني بظهور الهجمات السيريانية والتي حدثت بسبب عاملين أساسين:

الأول: باستحداث أجهزة الكمبيوتر في مُنتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً (Digital)، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.

الثاني: فهو ظهور الشبكة العنكبوتية "الإنترنت"، الذي أحدث انقلاباً مشيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى أطلق البعض عليها مُصطلح الحرب السيبرانية الباردة "Cyber Cold War" أو سباق التسلح "Cyber arms race".

المبحث الثاني: الأمن السيبراني الأهمية والأبعاد

يُعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية.

ويتميز الأمن السيبراني بمجموعة من الخصائص منها:

- أ. انه طابع مُتعدد التخصصات الاجتماعية والتقنية.
- ب. كونه شبكة خالية من الحجم والتي قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
- ت. درجة عالية من التغيير والترابط وسرعة التفاعل.

الأمن السيبراني: الفواعل والأبعاد

يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية: أ. الدول: والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها، فالدولة هي الفاعل المحوري بامتياز في

هذا العام الافتراضي لما لها من مكانة على أساس التفوق التكنولوجي والمؤهلات التي ترشحها لتبني هذه المكانة.

ب. الفواعل غير الدولاتية: ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية، وتشمل هذه الفواعل ما يلي:

ت. الشركات المتعددة الجنسيات: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فـ **Google**، **Facebook**، و **مايكروسوفت Microsoft**، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

ث. المنظمات الإجرامية: تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم "**Dark internet**" لتجارة المخدرات والأسلحة، والاتجار بالبشر.

ح. الجماعات الإرهابية: تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة، وتدريب المجندين الجدد

عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيراني حقيقي على منشآت البنية التحتية للدول.

خ. الأفراد: أصبح الفرد بفضل الفضاء السيراني فاعلاً مؤثراً في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكيليكس "Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

أبعاد الأمن السيراني:

يطال الأمن السيراني جميع المسائل العسكرية، الإقتصادية، والإجتماعية، والسياسية، والإنسانية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيرانية وعليه البد من توضيح أبعاد الأمن السيراني، التي هي الآتية:

- البعد العسكري :

يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها، وهي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الإنترنت وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيداً من الإختراق الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الإتصال بين القيادة والوحدات العسكرية فضلاً عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة "طائرات بدون طيار، صواريخ موجهة أقمار صناعية" ويعتبر فيروس

ستاكسنت "Stuxnet" بداية الاستعمال للقوة السيبرانية لتدمير البنية املادية هاجم حواسيب أجهزة الطرد المركزي الإيرانية.

كذلك، ترد هنا اختراقات أنظمة المنشآت النووية في إيران، وتحقق إمكانات التلاعب بها، مع ما يعنيه ذلك من تهديد للأمن القومي، للدولة المعنية، ومن تعرض السلم الدولي للإهتزاز، في ضل هذا المجال أي يمكن إيراد الأختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ما بين الاشخاص، والمؤسسات، والمصالح، في هذا السياق وجه خبراء أمريكيون، خطاباً مفتوحاً إلى الرئيس الأمريكي، "جورج بوش"، في أيلول 2011، محذرين إياه من خطر الهجمات السيبرانية على البنية التحتية الأميركية، التي تضم إلى الدفاع، امدادات الطاقة الكهربائية والمياه والاتصالات السلكية واللاسلكية والخدمات الصحية، والنقل والإنترنت. (زرزوقه، 2019)

البُعد الاجتماعي :

يفوق مستخدمو الإنترنت 4 مليارات شخص في العالم، وأكثر من 6.2 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة لكن في المقابل يعرض اخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الإنترنت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فالبد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي، سمح طبيعة الإنترنت المفتوحة، عبر المدونات والشبكات

الاجتماعية بشكل خاص، لكل مواطن، بأن يعبر عن تطلعاته السياسية، وطموحاته الاجتماعية، بأشكالها كافة، كذلك، تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة إغناء هذا المجتمع وتطويره، بما تتيحه من فرص للاطلاع على الأفكار، والمعلومات، المختلفة وبما تكونه من حاجة لدى الجميع، في الحفاظ على استقرار الأمن السيرياني، والمجتمع الذي يركز إليه والمعلوم، إن انفتاح مجتمع ما، على مجتمع آخر، يؤسس لتبادل خبرات، وأفكار، وتكون حاجات جديدة وآفاق تعاون وتكامل، يضاف إلى ذلك، ما تقدمه شبكة الإنترنت، من إمكانات وقدرات، للمجالات العلمية والثقافية، وإلى فئات محددة، ككبار السن، والمرضى، والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، وغيرهم من ذوي الاحتياجات الخاصة.(زروقه،2019)

وهذا عدا عن الدور الذي يمكن أن تؤديه، في تبادل المعلومات، في أوقات للالزمات الإنسانية والكوارث بحيث تتأمن المساعدات، وتوزع بالسرعة المطلوبة، ولا تقف الأبعاد الاجتماعية، عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والأفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، إضافة إلى العادات والتقاليد، عبر إنشاء المجموعات، التي تهتم بنشر الوعي حول هذه المسائل.(زروقه،2019)

البُعد السياسي :

يعد التدخل الروسي السيرياني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيرياني في بُعدة السياسي، إضافة إلى التسيريات للوثائق الحساسة

والإختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيرياني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

وتتمثل الأبعاد السياسية للأمن السيرياني، بشكل أساسي، في حق الدولة في حماية نطاقها السياسي وكيانها، ومصالحها الاقتصادية، التي تعني، حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن، أن يتحول إلى لعب أساسي، في اللعبة السياسية، كما أصبح بإمكانه الإطالع، على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات، التي يمكنه الوصول إليها، أو التي يمكن أن توزع وتنشر على الإنترنت، وبقية الأجهزة التي توصل به، بالمقابل، لا يتوانى العاملون في الشأن السياسي عن الافادة مما تقدمه هذه التقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين، والترويج لسياساتهم، في العالم، وغني عن البيان، مدى التأثير الذي يتركه هذا الأمر، بغض النظر عن صحة السياسات، والمبادئ والمواقف، التي يروج لها، فقد استخدم أوباما، مثلاً، الشبكات الإجتماعية بشكل كثيف، خلال حملته الانتخابية، كما تركت التسريبات، آلاف الوثائق الدبلوماسية السرية، عبر الويكيليكس، أثر سلبياً على العلاقات بين الدول، وعلى مصداقيته.

البُعد القانوني:

يرتب النشاط الفردي والمؤسسي والحكومي، في الأمن السيرياني، كما أسلفنا، نتائج قانونية، وموجبات تستدعي اهتماماً، لجهة إيجاد القواعد الخاصة، بحل

النازعات التي يمكن أن تنشأ عنها، لذا، لا بد من مراعاة بعض التحولات، التي رافقت ظهور مجتمع المعلومات، فيإلى الحقوق الأساسية، والحريات الإنسانية المعترف بها، في الدساتير والتشريعات الدولية، أضيفت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية والحق في إنشاء التجمعات على الإنترنت كما الحق في حماية ملكية البرامج المعلوماتية.(زروقه،2019)

وإن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للامعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان الى الاطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحته الفرق بين أمن المعلومات والأمن السيبراني.

البعد الإقتصادي:

يرتبط الأمن السيبراني، ارتباطاً وثيقاً بالإقتصاد، فالتزامن واضح، بين اقتصاد المعرفة، وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، المخزنة والمستخدمة، على كل المستويات، كذلك، تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الإقتصادية لبلدان كثيرة، عبر إفادتها، من فرص الإستخدام، التي تقدمها الشركات الدولية، والشركات الكبرى، التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط، الا أن هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل، أو بحماية المستهلك على الإنترنت. (زروقه ،2019)

ويضاف إلى ذلك، دخول العالم عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي وتتنافس الشركات، على إصدار تطبيقات، تسمح بآليات دفع آمنة، ويحفظ المال في المحفظة الإلكترونية، وبالبقاء من خلالها، وباستخدامها كرسيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال وغني عن القول، ما يمكن أن يثيره هذا الأمر من صعوبات.

الفرق بين الأمن السيبراني وأمن المعلومات

يعتبر الأمن السيبراني وأمن المعلومات مفهومين هامين للغاية في مجال التكنولوجيا واصبحا يستخدمان كثيرا هذه الايام , لكن الكثير من الناس الذين يستخدمونها يخلطون بينهما او يستخدمونهما كأنهما نفس الشيء لهذا لا بد من بيان الأمن السيبراني وأمن المعلومات.

يعتبر أمن المعلومات من المجالات التي تهتم بحماية البيانات الرقمية او غير الرقمية من اي هجمات الكترونية او استخدام غير مصرح به، كذلك يهتم بشكل اساسي بحماية المعلومات مهما كان نوع او شكل هذه المعلومات كما ان أمن المعلومات يهدف الى تحقيق المبادئ الاساسية التالية : (عطيف وقاسم 2019)

1 - السرية :

يهدف مبدأ السرية الى جعل المعلومات حصرية فقط للذين لديهم التصريح بالوصول اليها وحجبها عن اي شخص لا يسمح له برؤيتها من خلال تشفير المعلومات او اي طرق اخرى.

2 - السلامة او النزاهة :

وهذا المبدأ يختص بحماية المعلومات من ان يتم تعديلها من قبل اشخاص غير مصرح لهم بذلك، فهو المبدأ الذي يحافظ على كون البيانات دقيقة ويمكن الاعتماد عليها.

3 - التوافر:

مبدأ التوافر هو الذي يهتم بجعل المعلومات متوافرة للأشخاص الذين لديهم تصريح بالوصول اليها وهذا في اي وقت يحتاجونها فيه. فهو الذي يتعامل مع الحفاظ على المعلومات موجودة وغير محجوبة لأي طرف من الأطراف المصرح لهم بالوصول اليها في اي وقت . والجدير بالذكر أن الثلاثة مبادئ السابقة الخاصة بأمن المعلومات قد انضم لها ثلاثة مبادئ اخرى جديدة هي :

أ. عدم التنصل :

ينص هذا المبدأ على عدم قدرة طرف على انكار استلامه للمعلومات، أو أنها لم تحول اليه، حيث من خلال التشفير نضمن أن الراسل قد حول المعلومات الى المرسل اليه ولا أحد غيره، ومبدأ عدم التنصل يتحقق بعد ان يتم تحقيق مبدئي السلامة أو النزاهة والأصالة .

ب. الأصالة :

مبدأ الاصالة هو المعني بالتأكد من أن المرسل اليهم هم الاشخاص الحقيقيين الذين نود ارسال المعلومات اليهم وليسوا منتحلين لشخصيتهم، وهذا المبدأ نفسه

يحدث عندما يتم ارسال العملات الرقمية "كالبيتكوين" من شخص إلى آخر من خلال المحافظ الرقمية .

ت. المسؤولية:

مبدأ المسؤولية هو المبدأ المعني بتتبع أفعال الأشخاص الذين وصلوا الى هذه المعلومات، وذلك لضمان معرفة من قام بتغيير أو بتعديل اي جزء من المعلومات والاحتفاظ بسجل للأفعال هذه للعودة اليها في اي وقت.

ومن أهم الاجراءات التي يقوم متخصصي أمن المعلومات باستخدامها :-

أ. تقوية كلمات السر.

ب. المصادقة الثنائية أو متعددة العوامل.

ت. التحكم بصلاحيات الوصول .

ث. التشفير .

ج. المسؤولية القانونية .

خ. التوعية والتعليم .

وبشكل عام يقوم المتخصصين بالتعرف على المعلومات وعلاقتها ببعضها البعض ومن ثم يقومون بتقييم تأمينها والثغرات والمشاكل الخاصة بها وأثرها على الوصول غير المصرح به.

كذلك يقومون بتقييم المخاطر وبوضع الاستراتيجيات التي سيتم التعامل بها مع الاختراقات أو الهجمات الإلكترونية .

ومن أهم المخاطر التي يتعامل معها أمن المعلومات:

- أ. استخدام تقنيات وأجهزة لها معامل أمان ضعيف.
- ب. اتلاف البيانات الرقمية وغير الرقمية.
- ت. مشاكل التشفير.
- ث. حدوث هجمات تستهدف النطاق الجغرافي أو موجهة جغرافيا.
- ج. برامج الحماية الضعيفة أو غير المتطورة خاصة عند التعامل مع البيانات الضخمة.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحالي وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني، كبُعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال، ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في العلاقات الدولية.

أهمية الأمن السيبراني

للأمن السيبراني أهمية كبيرة في كافة المجالات تتمثل فيما يلي:

- (1) توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها، وذلك بعدم السماح لغير المخولين بالوصول إليها وإستخدامها.
- (2) الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيدي من العبث بها.
- (3) تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.

(4) حماية الأجهزة والشبكات ككل من الإختراقات لتكون درع واقٍ للبيانات والمعلومات.

(5) إستكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

(6) إستخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيرياني.

(7) توفير بيئة عمل آمنة جداً خلال العمل عبر الشبكة العنكبوتية.

عناصر الأمن السيرياني

حتى يتحقق الهدف من الأمن السيرياني، لا بد من توفر مجموعة عناصر تعمل مع بعضها البعض لتكمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيرياني:

1. التقنية: تشكل التكنولوجيا والتقنية دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيريانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالإعتماد على جدران الحماية وإستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

2. الأشخاص: يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما إستخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفاذي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.

3. الأنشطة والعمليات: يتم توظيف الأشخاص، والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني، والتصدي لهجماته بكل كفاءة.

معايير الأمن السيبراني الوطني:

للأمن السيبراني معايير عدة تتمثل فيما يلي: (التميمي، 2021)

أ. إقامة علاقة تعاونية وطنية بين المجتمعات المعنية بصناعة الاتصالات والمعلومات.

ب. التصدي للجريمة السيبرانية وردعها ومنع وقوعها.

ت. ترسيخ جذور الثقافة المتعلقة بالأمن السيبراني وتحفيزها.

ث. العمل ملياً على تطوير الإستراتيجيات الوطنية ذات العلاقة وتوفير الحماية الفائقة للبنية التحتية لأكثر المعلومات حساسية

ويحمل الفضاء السيبراني تأثيره في مختلف مجالات الحياة ومنها المجال الأمني حيث يساهم الفضاء السيبراني ومن خلال ادواته المختلفة في إعادة رسم البعد الأمني المحلي والعالمي، حيث يعمل على إعادة تشكيل الوعي والادراك السياسي والأمني للأفراد والمجتمعات والدول بصورة مغايرة عما كانت عليه حيث نجد تصورات وبنى جديدة يتم تأسيسها في المجال السياسي والأمني حيث لم يعد الأمن يعيش في العالم الواقعي المحدود، وأما أصبح للا واقعية واللامحدودية التي يشكلها الفضاء السيبراني حضورها المؤثر في المجال الأمني، وأصبح الحديث عن الحرب السيبرانية والأمن السيبراني والردع السيبراني والجيوش السيبرانية والأسلحة السيبرانية والإرهاب السيبراني والجريمة

السيبرانية، وغيرها، واتجهت الدول نحو تأسيس مؤسسات بحثية وامنية تهتم بدراسة الفضاء السيبراني وكيفية توظيفه بالشكل الذي يساهم في تحقيق مصالحها السياسية والأمنية والاقتصادية، ليكون التحدي المستقبلي الذي يفرضه الفضاء السيبراني يتمثل في قدرة الدول على التكيف مع التغيير السريع والتحديات التي يفرضها الفضاء السيبراني في المجالات العامة عموماً، والمجال الأمني خصوصاً إلى جانب امتلاك القدرات والبنى المادية والبشرية التي تمكنها من ان تكون مؤثرة وفاعلة فيه، وهذا التأثير الذي يحمله الفضاء السيبراني في المجال الأمني لا يقتصر على الواقع الداخلي للدول، وانما يمتد الى المحيط الدولي الواسع ليوثر في إعادة رسم شكل ومضمون الأمن الدولي، ويحدد اطرأً جديدة لطبيعة العلاقات الدولية والأمن الدولي.(التميمي، 2021)

وسائل التواصل الاجتماعي والأمن السيبراني

لقد تحول دور وسائل الإعلام الاجتماعي للأمن السيبراني إلى غمط حياة لبعض الأفراد، خاصة انه يتم إستخدامها للبقاء على اتصال، والتخطيط للمناسبات، وتبادل الصور لدينا والتعليق على التطورات الأخيرة وقد حلت محل البريد الإلكتروني والهاتف يتطلب طن منا، ومع ذلك، كما هو الحال مع أي شيء آخر على شبكة الإنترنت، فمن الضروري أن يكون هناك معرفة عن المخاطر، وأجهزة الكمبيوتر والهواتف المحمولة والأدوات المختلفة هي أصول لا تقدر بثمن التي تزود الناس من أي عمر مع قدرة غير عادية على الاتصال والتعاون مع كل ما تبقى من العالم، ويمكن للأفراد القيام بذلك بطرق مختلفة، بما في ذلك استخدام وسائل الإعلام الاجتماعية، أو مواقع الشبكات من باب المجاملة من وسائل الاعلام

الاجتماعي ويمكن للناس مشاركة التأمّلات والصور والتمارين، أو أي جزء من حياتهم على أنها يمكن أن تجلب نظرة غير معروفة في حياة الآخرين، بغض النظر عما إذا كانوا يعيشون في مكان قريب أو في جميع أنحاء العالم، إلا أنه ولسوء الحظ، تمثل هذه الشبكات بالإضافة إلى ذلك الأمان تجاه جهاز الكمبيوتر الشخصي والحماية وحتى أمانها، وجمع وسائل الاعلام الاجتماعية ترتفع كما هو خطر الاعتداء على مواقع وسائل الاعلام الاجتماعي التي تستخدم تقريبا من قبل معظمهم الناس، فقد أصبح مرحلة ممتازة لمُجرمي الإنترنت لاختراق البيانات الخاصة، وأخذ بيانات هامة. (Kalakuntla & others, 2019)

الفصل الثاني

التحديات والجريمة السيبرانية

لقد كان لظهور الإنترنت والثورة المعلوماتية دوراً في بزوغ العصر السيبري، وخلق بيئة جديدة، سميت بالفضاء السيبراني، وقد أصبح هذا الفضاء يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة السيبرانية، والتي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، الأمر الذي جعل الفضاء السيبراني مجالاً جديداً للصراع بين الدول.

لقد أدى ظهور الفضاء الإلكتروني واستخداماته في كثير من المجالات إلى تغيير شكل وطبيعة عمل النظام السياسي، حيث لعب دور المؤسسات الوسيطة والتواصل مابين عملية صنع القرار والرأي العام، إضافة إلى أنه ساعد على نقل النشاط السياسي الداخلي إلى ظاهرة عالمية، من خلال التواصل بين دول العام المختلفة والانفتاح على التطورات الديمقراطية في العالم أجمع . (طالة، 2020)

إلا أن مخاطر السيبرانية قد تزداد كلما ازدادت هيمنة تكنولوجيا المعلومات والاتصال على النسق العام للحياة، فاصبحنا امام جرائم حقيقة ومتكاملة الاركان، تتم عن طريق شبكة الإنترنت بأشكال مختلفة كسرقة الاموال والنصب والاحتيال، والتخطيط للعمليات الإرهابية، فضلا عن ترويج الاخبار المضللة، والقرصنة باعتبارها الجريمة الأكثر شيوعاً في العالم الرقمي.

وفي هذا السياق، فإن البحث في مكونات الأمن السيبراني والتحديات الأمنية في العصر الرقمي بحاجة إلى الغوص فيها من أجل بيان بيئة التهديدات، خاصة أن شبكة الإنترنت توفر لحوالي مليار ونصف مواقع الكترونية وصفحات لا عدد لها، وخاصة

مع الانتشار الواسع فيما بعد العام 2018، واتصلاً بموضوع التهديدات السيبرانية تُشير تقارير عدة وإحصائيات إلى نحو حوالي 95% من الشركات الكبرى متعددة الجنسيات تعترف بتعرضها للقرصنة، حيث اتخذت أكثر من حوالي 135 حكومة في العالم إجراءات حازمة تخص العالم الافتراضي والأمن الإلكتروني، خاصة مع كثرة الاعتداءات الإلكترونية بين الدول.

ويمكن اعتبار تحدي الأمن السيبراني أعلى تحديات يواجهها الأمن القومي في القرن الواحد والعشرين خاصة أن الأمن لا يقتصر فقط على الجوانب العسكرية، بل فإنه يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة.

المبحث الأول: التهديدات السيبرانية

أدى النمو المتزايد للتكنولوجيا في مجال المعلومات والاتصالات أيضًا إلى تهديدات بأن الهجوم السيبراني هو مثال واضح على مثل هذا التهديد. إن عواقب مثل هذه الهجمات خطيرة للغاية لدرجة أن الجهات الفاعلة الدولية، ولا سيما الحكومات، سعت إلى تبني الإجراءات والمواقف السياسية والقانونية المناسبة. التحدي الأكثر أهمية في هذه القضية هو وضع تصور وتعريف للهجوم السيبراني والحاجة إلى شرح وتعريف النطاق المفاهيمي لهذه الظاهرة، والذي يختلف اختلافًا كبيرًا بين الممارسة الرسمية للدول والمنظمات الدولية، حتى الآن لا يوجد توافق في الآراء بشأن التعريف. لم يتم الحصول على هجوم ساير.

ويمكن القول إن هذا التهديد، نظراً لسماته مثل سعر الدخول المنخفض، وإخفاء الهوية والتأثير الهائل قد خلق ظاهرة تسمى انتشار القوة، والتي لم تتسبب فقط في زيادة قدرة الحكومات الصغيرة على ممارسة السلطة. في هذا المجال، ولكن أدى ذلك إلى دخول جهات فاعلة جديدة مثل الشركات والجماعات المنظمة والأفراد في معادلات القوة العالمية. لذلك، فقد أثرت هذه الظاهرة على الأمن القومي من حيث مفهوم الأمن والحكومة المركزية في الأمن، والبعد الجغرافي للتهديد، ومدى نقاط الضعف، وكيفية التعامل مع التهديدات وتعدد الجهات الفاعلة في هذا المجال.

واليوم، يلعب الإنترنت دوراً مهماً في الاتصالات العالمية ويتم دمجها بشكل متزايد في حياة الناس حول العالم. ومع ذلك، فقد فرضت الإنترنت تحديات أمنية جديدة على الحكومات. جعل انتشار الهجمات الإلكترونية عبر الحدود الأمن السيبراني أحد الاهتمامات العالمية الرئيسية في القرن الحادي والعشرين، ويعتبر توفير

الأمن ومكافحة الإرهاب من المهام الرئيسية للحكومات، وهو أمر مهم في الفضاء السيرياني بسبب طبيعة الفضاء السيرياني باعتباره قاعدة المعلومات الرئيسية للدولة، وإمكانية حدوث أي هجوم وحرب إلكترونية تهدد الأمن القومي، وتختلف التهديدات عن التهديدات التقليدية، فقد أصبحت مهمة للغاية. الهجمات الإلكترونية هي ظاهرة ناشئة بين الحروب الحديثة التي تهدد السلم والأمن العالميين.

أولاً: التهديدات السيريانية

يعد الأمن السيرياني إحدى أسرع الصناعات نمواً الآن، فقد أصبح عدد الأشخاص الذين يدركون أهمية حماية البيانات أكثر من أي وقت مضى، وقد انتبهت الشركات، وخصوصاً لأن الحوادث تكلف تلك الشركات مليارات الدولارات كل عام وتكشف وتنشر كمية هائلة من البيانات الشخصية المهمة.

وتتمثل أهم التهديدات للأمن السيرياني فيما يلي: (خطاب، 2021)

1- هجمات التصيد الاحتيالي والهندسة الاجتماعية:

عندما يخدع المجرمون الإلكترونيون الأشخاص للكشف عن معلومات حساسة ككلمات المرور وأرقام الضمان الاجتماعي، يُطلق على ذلك التصيد الاحتيالي. من أشهر طرق حدوث التصيد الاحتيالي أن يتلقى الشخص رسالة بريد إلكتروني تبدو ظاهرياً أنها من مصرف أو مؤسسة حكومية ويتم استدراجه إلى مواقع تبدو حقيقية. وبمجرد الوصول إليها، يُطلب من الشخص إدخال كلمة المرور وأرقام الضمان الاجتماعي والبيانات المالية.

ثم يأخذ المجرمون الإلكترونيون هذه المعلومات ويستخدمونها لأغراضهم الخاصة. يُعد التصيد الاحتيالي جزءاً من مشكلة أكبر تُسمى الهندسة الاجتماعية، التي

تتلاعب في الأساس بالعواطف من أجل كسب الوصول إلى البيانات الحساسة، فلا تتأثر بهذه الخدع، وتشكك في كل رسالة بريد إلكتروني تتلقاها، لا سيما الرسائل التي تطلب إعادة إدخال معلوماتك الخاصة، تذكر أن المصارف الحقيقية والمؤسسات الحكومية لا تطلب منك التحقق من أي معلومات من المحتمل أن تكون حساسة.

2- الطرف الثالث:

يستخدم العديد من تجار التجزئة أطرافاً ثالثة لخدمات، مثل معالجة الدفع، وعلى هذا النحو، يعتقدون في كثير من الأحيان أن المسؤولية عن اختراق طرف ثالث لا تنطبق عليهم، والواقع، أن استخدام بائع خارجي لا يعفيهم من المسؤولية عن اختراق البيانات.

حتى إذا لم تتعامل الشركة بشكل مباشر مع المعلومات الشخصية، ومن بينها أرقام الضمان الاجتماعي أو أرقام بطاقات الائتمان، فقد يعرضها طرف ثالث للخطر، وباستخدام البرامج الضارة، يمكن للقراصنة سرقة البيانات من خلال موردي الجهات الخارجية، كما فعلوا في هجوم البرامج الضارة المستهدفة في عام 2013 حتى إذا كان الهجوم قد نشأ مع طرف ثالث، فإن الشركة التي تعاقدت مع بائع الطرف الثالث لا تزال مسؤولة ومطلوبة قانوناً لإخطار عملائهم والمنظمين إذا كان هناك إختراق للبيانات، يمكن أن تكون الغرامات والعقوبات باهظة؛ تتراوح بين عشرات الآلاف وملايين الدولارات حسب الظروف.

3- إدارة التصحيح:

تبدأ العديد من الهجمات ببرامج قديمة، لهذا السبب، فإن عدم مواكبة أحدث تصحيحات البرامج يجعل الشركات عرضة لأي عدد من انتهاكات أمن المعلومات،

فبمجرد أن يعلم المهاجمون بوجود ثغرة أمنية في البرامج، يمكنهم استغلالها لشن هجوم إلكتروني، ويوضح هجومان إلكترونيان واسع النطاق تم إطلاقهما في مايو 2018 هذا الاتجاه في الأمن السيبراني، فقد استغلت الهجمات نقطة ضعف خطيرة في نظام التشغيل "Windows" المعروف باسم "Eternal Blue"، وبشكل حاسم، أصدرت "Microsoft" تصحيحًا لثغرة "Eternal Blue" قبل عدة أشهر، وقد تم ترك المنظمات التي لم تقم بتحديث برامجها مكشوفة، وضاعت ملايين الدولارات بسبب خطأ بسيط في تحديث البرامج.

4- نقاط الضعف في الخدمات السحابية:

كلما زاد الاعتماد على السحابة لتخزين البيانات، زادت مخاطر حدوث اختراق كبير، الخدمات السحابية معرضة لمجموعة واسعة من الهجمات الإلكترونية، يتضمن ذلك هجمات الاستيلاء على الحسابات ورفض الخدمة "DoS"، التي تمنع الشركات من الوصول إلى بياناتها، وتعتقد العديد من الشركات أنها آمنة لأنها تستخدم تقنية أمان السحابة، والواقع أن التكنولوجيا ليست سوى جزء من الحل، ونظرًا لأنه لا توجد تقنية يمكنها القضاء تمامًا على نقاط الضعف، فستظل هناك حاجة إلى نهج شامل لحماية قوية، ويعد التأمين جزءًا مهمًا من تلك الحماية كجزء من خطة شاملة لإدارة المخاطر الإلكترونية.

5- طلب الفدية:

تعد هجمات برامج الفدية تهديدًا إلكترونيًا خطيرًا، فعندما تصيب هذه الهجمات شبكة ما، تحتجز بياناتها وأنظمة حواسيبها رهينة حتى يتم دفع فدية، والخسائر الفورية من الفدية لا تكون سوى غيض من فيض وغالبًا ما تكون الأضرار المالية الناتجة عن

فقدان الإنتاجية وفقدان البيانات هي الأكثر تدميراً للأعمال التجارية مثل هذه الهجمات هي السبب في خروج 60% من الشركات الصغيرة من العمل في غضون 6 أشهر من الاختراق الإلكتروني، وتعتبر برامج الفدية من بين أكبر 10 أنواع من الهجمات الإلكترونية، وهي طريقة شائعة للمهاجمين لاستهداف الشركات، ولن يتغير هذا قريباً؛ وفقاً لوزارة الأمن الداخلي الأمريكية وستتزايد هجمات برامج الفدية في جميع أنحاء العالم، وقد سلطت الهجمات السيبرانية لطلب فدية الضوء على الحاجة إلى أشياء مثل حماية نقطة النهاية للمساعدة في تقليل الانتشار اللاحق وتسريع أوقات الاستجابة، والمصادقة متعددة العوامل "MFA" للوصول عن بُعد إلى نقطة لإيقافها المحتمل والتطفل قبل حدوثها، بالإضافة إلى فصلها واختبرت النسخ الاحتياطية، لذا عند حدوث حدث فدية، يمكنك الاسترداد بسرعة.

6- الخطأ في الامتثال للحماية:

إن تلبية معايير امتثال البيانات ببساطة ليست ماثلة للحماية المستمرة والقوية، فعلى سبيل المثال، يحتاج العديد من الشركات إلى تلبية معيار أمان بيانات صناعة بطاقات الدفع "PCI DSS" للتدقيق السنوي، ومع ذلك، فإن هذا لا يمثل بالضرورة معيار الحماية المعتمد، فوفقاً لتقرير الامتثال "PCI" لشركة Verizon فشلت أربع من كل خمس شركات في الحفاظ على الامتثال في تقييمها المؤقت، وكانت هذه هي نفس الشركات التي استوفت معايير الامتثال سابقاً، ولا تزال الشركات التي تم اعتبارها متوافقة مع معايير "PCI DSS" تعاني من انتهاكات الأمن السيبراني، بعد أسابيع قليلة من اعتمادها، كما علمت هذه الشركات، فإن استيفاء المعايير القانونية المناسبة ليس بديلاً عن الحماية الإلكترونية.

7- مهددات أمن الأجهزة المحمولة:

يمكن أن تكون تكنولوجيا الهاتف المحمول أحد الأصول المهمة للشركات، ولكنها قد تعرضها أيضاً لانتهاكات محتملة للأمن السيبراني، وقد خلصت النتائج الواردة في تقرير لأمان الأجهزة المحمولة إلى أن واحدة من كل 5 مؤسسات تعاني من انتهاكات أمان تلك الأجهزة، وجاءت غالبية هذه الهجمات من البرامج الضارة وشبكات "Wifi" الخبيثة، ويمكن للمُجرمين الإلكترونيين استغلال الثغرات الأمنية في هاتفك المحمول بسهولة للحصول على البيانات الخاصة، وتتولد هذه الثغرات الأمنية أحياناً من التطبيقات التي تستخدمها أو من هاتفك الذكي نفسه، وتقع الهواتف المحمولة كذلك عرضة للإصابة بالبرامج الضارة، والتي يمكنها تسجيل ضغطات المفاتيح والتقاط لقطات للشاشة، فلا بد من حماية الخصوصية عن طريق فحص التطبيقات التي تنزلها وتوخي الحذر تجاه رسائل البريد الإلكتروني التي تفتحها والصور التي تقرر تحميلها.

8- سياسات "أحضر جهازك":

تشجع العديد من الشركات الموظفين على استخدام الأجهزة الشخصية في العمل كجزء من سياسات أحضر جهازك الخاص، وهذا له العديد من الفوائد من بينها زيادة المرونة والراحة، حتى إن البعض يزعم أنه يساعد على زيادة الإنتاجية والروح المعنوية، ومع أن هناك العديد من الفوائد، يمكن لسياسات "أحضر جهازك" أن تعرض الشركة لانتهاكات خطيرة للأمن السيبراني، ويمكن أن يكون اختراق الأجهزة الشخصية أسهل من اختراق أجهزة الشركة، مما يخلق فرصة للمهاجمين لاختراق الشبكات وتعريض البيانات للخطر، ولذلك من المهم مراجعة هذه السياسات والتأكد من تدريب الموظفين بشكل صحيح لتقليل المخاطر الإلكترونية المرتبطة بها.

9- إنترنت الأشياء:

يربط إنترنت الأشياء الأجهزة من جميع أنحاء العالم عبر الإنترنت، ويسمح هذا بشبكة من الأجهزة يمكنها تخزين البيانات وإرسالها واستلامها، يستفيد منه العديد من الأفراد والشركات من إنترنت الأشياء بسبب ملاءمته، لكن الشيء الذي يجعلهم مناسباً يجعله أيضاً معرضاً للخطر، ويمكن للقراصنة استغلال الاتصال بالإنترنت كنقطة وصول لسرقة البيانات، ونظراً لاعتماد الشركات بشكل متزايد على أجهزة إنترنت الأشياء يتوقع العديد من الخبراء أن يكون هذا أحد أكبر التهديدات السيبرانية في السنوات القادمة.

10- الأجهزة التي عفا عليها الزمن:

لا تأتي جميع التهديدات للأمن السيبراني من البرامج، فالوتيرة التي يتم بها إصدار تحديثات البرامج يمكن أن تجعل من الصعب على الأجهزة مواكبة ذلك، وهذا بدوره يؤدي إلى تعرض بيانات الشركات للخطر، وإذا أصبحت الأجهزة قديمة، فلن تسمح العديد منها بالتحديثات بأحدث التصحيحات والتدابير الأمنية، والأجهزة كذلك التي تعتمد على البرامج القديمة أكثر عرضة للهجمات السيبرانية، مما يخلق ثغرة أمنية كبيرة محتملة، ومن المهم مراقبة ذلك والاستجابة بسرعة عندما تصبح الأجهزة قديمة، وكما يجب أن تحافظ على تحديث برامجه، يجب أن تفعل الشيء نفسه مع الأجهزة.

11. سرقة الهوية.

تعد سرقة الهوية إحدى أسرع جرائم الإنترنت تطوراً، ويمكن أن تؤدي العديد من النقاط السالفة من قبل إلى سرقة الهوية، ومنها رسائل البريد الإلكتروني للتصيد

الاحتياالي وعمليات اختراق البيانات ومع ذلك تبقى هويتك عرضة للخطر أيضًا من خلال المواد اليومية كسيرتك الذاتية وعنوان منزلك والصور ومقاطع الفيديو عبر مواقع التواصل الاجتماعي والبيانات المالية، وغيرها، سيسرق سارقو الهوية المعلومات الشخصية ويفتحون بطاقات ائتمان وحسابات للقروض باسمك، وفي حين أن بعضاً من هذا يقع خارج نطاق سيطرة الشخص العادي، لا يزال أمامك الكثير الذي يمكنك القيام به للحفاظ على أمن هويتك.

12. تهديدات أمن الأجهزة المحمولة والثغرات الأمنية في الهواتف الذكية

يُمكن للمجرمين الإلكترونيين إستغلال الثغرات الأمنية في هاتفك المحمول بسهولة للحصول على البيانات الخاصة. وتتولد هذه الثغرات الأمنية أحياناً من التطبيقات التي تستخدمها أو من هاتفك الذي نفسه. تقع الهواتف المحمولة كذلك عرضة للإصابة بالبرامج الضارة، والتي يمكنها تسجيل ضغطات المفاتيح والتقاط لقطات للشاشة، لذلك لا بد من حماية نفسك عن طريق فحص التطبيقات التي تنزلها وتوخي الحذر تجاه رسائل البريد الإلكتروني التي تفتحها والصور التي تقرر تحميلها. (<https://me.kaspersky.com/resource-center/threats/top>)

13. اختراقات بيانات البيع بالتجزئة

تشكل اختراقات بيانات البيع بالتجزئة خطورة حقيقية حيث يمكن أن تؤثر فعلياً في أي شخص، وقد شهد عام 2014 ارتفاعاً في الهجمات الإلكترونية التي تستهدف الشركات الكبيرة، حيث سرق المتطفلون أرقام بطاقات الائتمان والسحب الخاصة بحوالي 40 مليون عميل، ويقوم المجرمون الإلكترونيون بسرقة هذه المعلومات الشخصية وبيعها في السوق السوداء، مما يمكن أن يؤدي إلى سرقة الهوية بسهولة.

وبينما تتحمل شركة البيع بالتجزئة جزءًا كبيرًا من المسؤولية، كأن تتولى تحديث أساليب الدفع وتأمينها، تبقى مراقبة حسابك المصرفي وكشف حساب بطاقة الائتمان الخاصة بك عن كُتب طريقة جيدة للحفاظ على أمنك أثناء الهجمات على البيع بالتجزئة. ([https://me.kaspersky.com/resource-center\(/threats/top](https://me.kaspersky.com/resource-center(/threats/top)

آليات مواجهة التهديدات السيبرانية

تشكل تلك التطورات للقدرات التكنولوجية والإلكترونية للدول في ميدان القوة السيبرانية، مكوّنًا رئيسيًا من مكوّنات مناعتها على الصّاعدين المحلي والعالمي، ومما لا شك أن أمنها القومي يتأثر سلبًا وإيجابًا من خلال جملة من الاستراتيجيات القومية الواجب توفرها تجنّبًا لأي طارئ قد يرهّن أمن تلك الدول القومية، وفي أي لحظة وتصبح تلك الدول عرضة للمساومات والتنازلات المفروضة، لذلك فالانفتاح على المعرفة والاستعانة بتكنولوجيا المعلومات والاعتماد المتزايد على أنظمة الحواسيب المتطورة وامتلاك القوة السيبرانية في العالم تقف أمامه جملة من التحديات الجديدة التي تتطلب أخذها بعين الاعتبار على المستوى الوطني أو الدولي: (فلاك، 2021)

أ. التحديث الإلكتروني المتواصل للأجهزة والمعدات الإلكترونية الحساسة والسرية.

ب. تطوير الترسانة الإلكترونية للدول وعصرنتها لتكون في مستوى المنافسة الدولية.

ت. تدريب الكفاءات الوطنية المتخصصة في مجال الرقمية، ورسكلتها بشكل مستمر ودوري.

ث. اعتماد جملة من القوانين والتشريعات الصارمة لمواجهة تلك الاختراقات الإلكترونية والقرصنة

ج. تطوير استراتيجية وطنية للأمن السيبراني من أجل حماية المعلومات والبيانات للدولة وللأفراد ومواجهة التهديدات السيبرانية المحتملة.

ح. التوعية المستمرة للموظفين داخل المؤسسات الرسمية بقواعد استخدام قواعد بيانات المواطنين، وتنمية المعايير المهنية الاحترافية لديهم، مقابل تشديد العقوبات ضد عمليات النسخ أو نقل أو تسريب البيانات.

خ. ضرورة إرساء بنية تحتية للدول بشكل ثنائي أو متعدد الأطراف من أجل صناعة البرمجيات عالية التقنية، ومحصنة ضد الإختراقات الإلكترونية والقرصنة المتكررة.

لقد تحوّل مفهوم الصراع الدولي في الفضاء الإلكتروني، من خلال تأثير التكنولوجيا الرقمية المتطورة بشكل لافت على استخدامات مفهوم القوة التقليدية في الصراعات الدولية المختلفة وخاصة في مجال الحروب السيبرانية، فكثير من الدول تسعى لدخول مجال التسابق والتنافس في امتلاك القوة السيبرانية من خلال الفضاء الإلكتروني، واستعمالها كأداة للصراعات الدولية وتحقيق مكاسب وانتصارات متنوعة على الصعيد السياسي أو الاقتصادي والعسكري باستعمال تلك التكنولوجيا الرقمية المتطورة، وبذلك انتقلت الفواعل الدولية من مستوى الحروب والتهديدات الأمنية الكلاسيكية إلى مستوى حروب وتهديدات من نوع مختلف، وهي الحروب والتهديدات السيبرانية، ومن جملة النتائج: (فلاك، 2021)

1. الصراع الإلكتروني للدول أحد أوجه الصراع التقليدي، الذي يهدد الأمن الدولي وأمن الدولة الواحدة والذي يستطيع أن يخلف خسائر فادحة كبيرة لها، ويتسبب في شل البنية المعلوماتية والاتصالية والرقمية للدولة المستهدفة عن طريق امتلاك تلك القدرات التكنولوجية والسيبرانية كبرامج التجسس والفيروسات.

2. لقد أصبح المفهوم الجديد للأمن القومي خلافاً للمفهوم التقليدي يهدف للحفاظ على سلامة الدولة والأفراد في ظل تلك التطورات التكنولوجية والرقمية السريعة والمتطورة، ومن ثم اختلفت آليات التعامل معها وأصبح الأمن انعكاساً للمسار التاريخي الذي عرف تطورا تصاعديا، وذلك انعكس على طبيعة الصراع الدولي الراهن مع الموجة المعلوماتية الجديدة التي يشهدها العالم، والتي تأثرت بتكنولوجيا المعلومات والفضاء الأزرق، والذي غير طبيعة الصراع والقوة التقليديين وممارستها على الصعيد الدولي، وبذلك أحدث جملة من التغييرات داخل البيئة الأمنية للنظام الدولي الراهن.

3. اتجه الصراع الدولي الراهن نحو التنافس في ساحة الإنجازات الاقتصادية والنجاحات التجارية وزيادة الصادرات، وامتلاك الأفكار والإبداعات المتنوعة واكتساح الأسواق العالمية، ذلك كله من خلال اكتساب المعلومات والبيانات والأسرار بالاستعانة بالقوة السيبرانية التي تمتلكها بعض الدول لاختراق تلك الأسرار الاقتصادية والتقنية والعلمية والتجارية للدول الأخرى من أجل تحقيق التنمية، ورفع معدلات النمو الاقتصادي لها.

4. إنَّ ظهور الإرهاب الدولي الجديد الذي يوظف تكنولوجيا الاتصال والمعلومات يعتبر من أخطر التهديدات الأمنية الجديدة التي تهدد أمن الدول والمجتمعات على حد سواء، ويختلف تماماً عن الإرهاب التقليدي، وذلك من خلال خصائصه وآثاره وطبيعة أطرافه، وإمكانية استخدامه للقوة السيبرانية كتهديد مباشر والاستعمال المفرط لكل البرامج المتطورة في مجال الفضاء الإلكتروني، واستعمالها في كافة أنشطته الحساسة، والتي تهدد الأمن الدولي والعالمي كالإرهاب النووي والبيولوجي والكيميائي.

وتشمل التهديدات السيبرانية عدة عناصر هي الآتية :

أولاً: الأمن الدولي :

يُعتبر الفضاء السيبراني ساحة جديدة بدايةً على مفهومي الفضاء السيبراني وعن الإرهاب الإلكتروني بحيث لا توجد تعريفات دقيقة بشأنهما. ففي مفهوم الفضاء السيبراني، نجد تعريفات عدة يتناول معظمها مكوناته من أجهزة الكمبيوتر والوسائط التكنولوجية وشبكة الإنترنت، في حين أنه يتضمن أيضاً العنصر البشري أو المعنوي، وتشير كلمة "Cyber" أو "Cybernetics" إلى "نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم محاكاة الآليات لها"، بالتالي فالمجال دراسة الاتصالات والتحكم الآلي في النظم العصبية للكائنات الحية والسيبري يتضمن "كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات، وتعرف كليات الحرب الأمريكية الإرهاب السيبراني، أو كما تسميه "هجمات الشبكات الكمبيوترية" انطلاقاً من تصنيفه تحت بند "العمليات الإلكترونية، وهو

يندرج في إطار الحرب الرقمية والتي عرفت من خلال الاجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها".

والإرهاب الرقمي يستهدف أمن العمليات، سواء العمليات النفسية، الخداع العسكري، الهجمات الفيزيائية ومهاجمة شبكات الكمبيوتر، ولا يوجد إجماع حول تعريف الإرهاب السيبراني، لكنه يُشير عموماً إلى شكل جديد من أشكال الإرهاب يندرج في إطار الجرائم الإلكترونية، وقد ه من استخدام وسائل تأخذ تسمى ووسائط التكنولوجيا المعلوماتية والاتصالية في تنفيذ أعمال إرهابية لها الأبعاد المحلية والوطنية لتؤثر بشكل كبير على الأمن الدولي، تتجاوز تداعيات، ويتضمن الإرهاب الإلكتروني أو الرقمي بهذا المعنى أعمال اختراق المواقع وأنظمة المعلومات، القرصنة، نشر الرعب وأشكال التهديد الموجهة نحو الافراد أو الدول استقطاب الافراد للنخراط في التنظيمات الإرهابية.

لقد أفرزت العولمة مجموعة من التطورات وتحديداً على الصعيد التكنولوجي والمعرفي، فحدث الدمج بين الفضاء السيبراني والأساليب، والتكتيكات المستخدمة في الصراعات الدولية، وأصبحت حرب المعلومات عمليات عسكرية تدور في ميدان تكنولوجي رفيع المستوى، بحيث تستخدم أطراف الصراع الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة وسائل تكنولوجيا المعلومات للحصول على الموقع الأفضل استراتيجياً، ذلك بالتوظيف الفعال لجميع الأسلحة المعلوماتية، ليصبح الإرهاب السيبراني بهذا المعنى تعبيراً عن صراع رقمي بين القيادات الصديقة والقيادات المعادية، بهدف التأثير على قدرات الخصم واختراق كيانه السيبراني ومهاجمة جهاز المعلومات المعادي وافشاله في إطار حرب المعلومات .

والحروب بهذا المعنى تختلف كثيرا عن الحروب التقليدية، بحيث أن الصراع في الفضاء بة أو المتوقعة مثال في ظلَ السبيرياني يظل محاطا بعلامات استفهام بخصوص النتائج المرتق محاولة السيطرة الكاملة على المؤسسات والهيكل الاستراتيجية للدول عن طريق استعمال أسلحة تكنولوجيا المعلومات والاتصالات أو مهاجمة المعلومات من خلال الوسائط الإلكترونية، وهو ما يؤدي في نهاية المطاف إلى شلل هذه الأنظمة والتهديد المباشر للأمن الوطني من خلال الهجوم على أنظمة صنع القرار والأنظمة الدفاعية للدولة والسعي إلى السيطرة على قواعد المعلومات، ومن ثم إمكانية حدوث رد فعل انطلاقاً من الحق الشرعي في الدفاع عن النفس، كما أن استهداف الاتصالات وأنظمة المواصلات والخدمات العامة للمواطن والدولة يمكن أن يؤدي إلى الأضرار بالحياة والممتلكات.

وتعتبر هجمات الفضاء السبيرياني أحد أنواع النزاع أو الصراع المسلح الأكثر ديناميكية، فهي تختلف عن أشكال النزاعات التقليدية، ويمكنها الحدوث بشكل غير مرئي وغير مشهود، مثل أن تقوم المخابرات الخاصة لاي دولة بشن هجمات باستخدام الأسلحة السبيريانية من أجل تخريب البنية التحتية المعلوماتية الخاصة بدولة أخرى. وتأتي هذه الملامح في نواحي الاستخدامات غير القانونية وغير المشروعة لهذا الفضاء، فضلا عما يمثله ذلك من تهديد للأمن الدولي في المجال السبيري والبنية التحتية الكونية لثورة المعلومات من جانب جميع الفاعلين في مجتمع المعلومات العالمي، خاصة التنظيمات الإرهابية والدول، والجماعات الإجرامية المنظمة، مما يطرح هواجس ويشكل تداعيات كبيرة على الأمن الدولي بصورة عامة.

ثانياً: مظاهر تهديد الإرهاب السيرياني للأمن الدولي

يمثل الفضاء السيرياني عنصر جذب مهم للتنظيمات الإرهابية على تعدد أنواعها واختلاف أيديولوجياتها نظراً لما يتيح من وسيلة إعلام دولية وسلاح في ذات الوقت، إذ يمكن استخدامه من قبل الأطراف المتعددة ويعد تنظيم "داعش" الإرهابي أكثر التنظيمات التي مثلت تهديداً حقيقياً لسلامة شبكة الإنترنت العالمية باستخدامها في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات الإرهابية، ووسيلة لحشد المتعاطفين معه، والمنتشرون في كثير من دول العالم، ويستخدم تنظيم "داعش" الإرهابي، والإرهاب السيرياني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة . (حكيم، 2018)

ومواقع التواصل الاجتماعي بغرض للتجنيد ونشر فكره في أوساط الشباب، والتي كان بإمكان عبر الإنترنت في بعض الأحيان أن تكون كافية لآثار أعمال العنف والخوف والرعب لدى الدول والمجتمعات، وفي هذا الإطار، يحدد "أبو بكر ناجي" في كتابه "إدارة التوحش" أساليب توظيف العالم الجهادي ضمن استراتيجية التنظيمات الإرهابية، وهي بالنسبة لتنظيم الدولة "داعش" تستهدف وتركز على فئتين:

فئة الشعوب: بحيث يتم العمل على دمج أكبر عدد منهم للانضمام إلى صفوف الجهاد و دعمها، من جهة أخرى، التعاطي السلبي مع من لا يلتحق بالتنظيم.

جنود العدو: خاصة أصحاب الرواتب الدنيا، للدفع بهم نحو الانضمام إلى صفوف المجاهدين أو على الأقل الفرار من خدمة العدو.

وقد عمل تنظيم "داعش" الإرهابي على تجنيد جيش إعلامي متخصص في العالم الإلكتروني، يعمل تحت تسميات مختلفة، مثل المراكز والمؤسسات والكتائب

العالمية، وهي على شكل شبكات بحيث تتواجد كل شبكة ضمن منتدى من منتديات "الجهادية" أو موقع من مواقع التواصل الاجتماعي، لدعم هدف من الاهداف التي يقرها العالم المركزي الخاص بتنظيم الدولة "داعش" الإرهابي مركز الفجر للإعلام، مؤسسة الفرقان العالمية كما أظهر تنظيم "داعش" الصور والفيديوهات من خلال مواقع التواصل الاجتماعي، بحيث يظهر فيها إرهاب التنظيم وهم يقطعون الرؤوس، فاحتوت مضامين الفيديوهات قدر كبير من الرعب والترويع في النفوس والصور على مشاهد عنف غير مسبقة، والغرض منها الافراد والمجتمعات والدول.

لقد استغلت الجماعات والتنظيمات الإرهابية، على شتى أشكالها وأنماطها الفكرية، تسهيلات عصر المعلوماتية والرقمية بوصفها عنصراً حيوياً لدعم وتحقيق أهدافها، ومنفذاً لوجيستيّاً داعماً وحاضناً للنشاط العالمي لها في مناطق مختلفة عبر العالم، بالتالي تشكيل مجتمع افتراضي خاص بها، يساعدها على الالتحام والتواصل الدائم، الذي يوهّم البعض بأن هذا المجتمع غير محدداً لإبعاد، وهو ما كان له دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات وقد ظهر الإرهاب إلى الإرهاب بأنه سلاح الضعيف الذي لا يقدر على تنظيم حرب ضد الدولة، فعن طريق الإرهاب يمكن إلحاق الذي ومحاولة هزيمة القوى العظمى، وهذا ما يتضح في الجماعات الاثنية والميليشيات العنصرية والأصوليات الدينية، وبعض الاقليات التي لا تمتلك القوة. (حكيم، 2018)

ويكون الإرهاب وسيلة لتأكيد الهوية وجذب الانتباه والأهتمام، فهو بالتأكيد وسيلة من وسائل الصراع الإرهاب السبيرياني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة يتعلق الإرهاب بالسموات المفتوحة والفضاءات التكنولوجية، ويكون وسيلة لتحقيق أهداف مستقبلية عبر تحطيم الحاضر للوصول

إليها بحيث يكون التحطيم بداية لظهور شيء معين من تحت ركامه، ويكون مدفوعاً بقيم أخلاقية أو ثقافة. (حكيم، 2018)

وينشأ الإرهاب إما بدافع الثأر وتوقيع العقوبة على أخطاء الماضي، أو القدرة على الإلهام والتبشير بعهد جديد، ففي الأول، يكون العنف استراتيجياً بشكل كبير، والأهداف محددة وواضحة، بينما الثاني يعبر عن كيفية تغيير العالم عن طريق الإرهاب، وبالرغم من تلك الاختلافات فإنها لا تعني بالضرورة وجود تمايزات في كل الأحوال .

إن الإرهاب بطبيعته ليس ظاهرة ثابتة، بل هو تهديد دائم التغير والتحول، بحيث يغير مرتكبه ملاحم ووسائلهم ليتكيفوا مع زمانهم ومواقفهم، ولضمان تحقيق ما يهدفون إليها، كما استفاد الإرهابيون من التطور التكنولوجي والثورة الرقمية بحيث أصبح بمقدورهم شراء المنتجات التكنولوجية التجارية والاستفادة مما تم إنفاقه في البحث والتطوير، فتمكنوا من الحصول على أجهزة كونية المدى وفائقة السرعة، متنوعة، معقدة ومشفرة وبدون أية تكاليف باهظة، وهو أمر منطقي إذ أتاحت شبكة الإنترنت الفرصة للحصول الكتساب المعلومات إصدار الأوامر والسيطرة على العمليات المخطط لها، وتمتلك الجماعات المتطرفة، بجميع أشكالها ومختلف توجهاتها السياسية، مواقع على شبكة الإنترنت وبشكل خاص شبكات التواصل الاجتماعي، ومنها ما يمتلك أكثر من موقع، يقدم خدماته بأكثر من لغة، كما هو شأن تنظيم الدولة "داعش"، من أجل التعريف بالتنظيم وتاريخه ومؤسسيه وأبطاله وأنشطته، وخلفياته السياسية والاجتماعية، وأهدافه السياسية والايدولوجية، وأحدث الأخبار ومضامين الانتصارات المحققة، كما أن رسائل المواقع تكون لها صور

متعددة، مثل الدعم الفكري لهذه التنظيمات وتبجيل أفرادها، أو مهاجمة المفكرين والشيوخ المعتدلين، أو مهاجمة الحكومات والأجهزة الأمنية ها يؤثر، وجميع على الأمن الدولي بكافة مستوياته وعلى جميع الأصعدة، قد تسعى تلك المواقع للتغطية على موقفها الداعم للإرهاب بالسماح بنقد يسير، والاستناد في ترويج فكرها إلى بعض الكتابات الأيدولوجية والدينية، والحاها بتفاسير معينة وقصص تاريخية وضعت ضمن تأويل متعسف لكي تقنع المتلقي بمشروعية عملها، بحيث يتم استغلال الدين باعتباره مظلة أيدولوجية تؤهل الاستقطاب عناصر جديدة، كما يتم نشر تلك التي دارتها من قبل أشخاص ذوي أفكار أحادية لا تسمح بوجود أحد يناقشها أو يعرض رأياً يخالفها.

ثالثاً: أنماط الجمهور التي تستهدفها رسائل المواقع الجهادية:

هناك عدة أنماط للجمهور التي تستهدف المواقع الجهادية وهي الآتية : (حكيم، 2018)

النمط الأول: هو جمهور المؤيدين الحاليين والمحتملين، وذلك عبر تقديم معلومات مفصلة حول أنشطة المنظمة الإرهابية وسياساتها الداخلية، والمحلية وحلفائها ومنافسيها، وعادة ما يكون هذا الجمهور جمهور.

النمط الثاني من الجمهور: هو الرأي العام العالمي، وهو الجمهور غير المتورط مباشرة في الصراع، ولكن لديه بعض المصالح في القضايا المطروحة، ويضم هذا الجمهور المستهدف الصحفيين ووسائل الاعلام التي تستخدم مواقع هذه التنظيمات للحصول على وجهات نظرها، يساعدها في ذلك طرح خدمات المواقع بلغات عدة.

النمط الثالث: يتمثل في الاعداء، وتسعى مواقع هذه التنظيمات إلى إضعاف معنوياتهم من خلال توجيه التهديدات، وتعزيز الشعور بالذنب لديهم إزاء الأفعال والدوافع.

أشكال الخطابات الدعائية التي تستخدمها الجماعات المتطرفة:

هناك عدة أشكال للخطابات الدعائية التي تستخدمها الجماعات المتطرفة: (حكيم، 2018)

الخطاب الأول: يتمثل في الدعاء بأنه ليس أمامها خيار إلا العنف الدموي بوصفه سوى التحول الذي يقى ضرورة أجبر عليها الضعيف للرد على العدو الظالم. ويتم تأكيد أعمال القوة التي تستخدمها الحكومات والأنظمة ضدها وضد تنفيذ مطالبها، كما يتم استخدام مصطلحات كالذبح والقتل والإبادة، وتصف التنظيمات المتطرفة نفسها من قبل القوى الكبرى أو دولة قوية بالمضطهدة والمطاردة، وهو ما يعطي انطبعا لدى جمهور المتعاطفين بأن التنظيم المتطرف والإرهابي ضحية.

الخطاب الثاني: يرتبط بشرعية استخدام العنف، فأعضاء الحركة أو التنظيم يعتبرون أنفسهم مقاتلين من أجل الحرية، ومجبرين ارادتهم على استخدام العنف، بما يتنافى وإل أن العدو يسحق كرامة نظر الشعوب وحقوق التنظيم ذاته، وأن عدو الحركة أو الجماعة هو الإرهابي الحقيقي.

الخطاب الثالث: هو الاستخدام الواسع لمبدأ العنف في محاولة لدرء الصورة العنيفة عن التنظيم بالمشاعر المتطرفة والإرهابي، بمعنى التمويه والتألق فعلى الرغم من كون تلك الجماعات جماعات عنيفة، فإن المواقع المرتبطة بها تدعي سعيها

للحلول السلمية، وأن هدفها النهائي هو التسوية الدبلوماسية 13 التي تتحقق عبر المفاوضات والضغط الدولي على النظم الجائرة .

وبرزت العلاقة ما بين الفضاء الإلكتروني والإرهاب من خلال عدد من المظاهر، لعل أهمها كونه أي هذا الفضاء سميت بخصائص تنافسية بشكل يجعله مسرح جذب الإرهابيين والقيام بإدارة الفكرة المدركة أو التحكم بالصورة المنطبعة " أي تصوير أنفسهم وأعمالهم بالضبط في الضوء والسياسات الذي يريدونه"، وسائل الاعلام الرسمية لذلك التصوير أو غربلته أو تحويله دون أن يعرقل ذلك تفح بدأ الإرهابيون بالفعل في استخدام الفضاء الإلكتروني في التأثير على الرأي العام، وتجنيده أعضاء جدد، وجمع الاموال.

واستخدم الإرهاب الفضاء الإلكتروني كوسيط علامي يتكون من أربعة عناصر: جهاز الارسال الإرهابي المتلقي المقصود الهدف، " الرسالة " التفجير، الكمين، " التغذية الإستراتيجية، ورد فعل الجمهور المستهدف ويمارس الإرهابيون في ذلك أشكالاً مكررة من استخدام اللغة المؤثرة، الهادفة إلى الاقناع شفويا وكتابيا وتصويريا، مما يرغب وسائل الاعلام على توفير الوصول إليها والذي بدوره لا يستطيع الإرهاب تحقيق أهدافه وتتألف كل وحدة إرهابية من أربعة أعضاء على الأقل: المرتكب، المصور، فني الصوت والمخرج لقد للجماعات الإرهابية عبر نشر رسائل الكراهية والعنف، وأصبح الفضاء الإلكتروني منبر، والاتصال ببعضها البعض ومؤيديها والمتعاطفين، وليست المواقع الإلكترونية سوى واحدة من خدمات الإنترنت التي سطا عليها الإرهابيون، فهناك تسهيلات عديدة أخرى كالبريد الإلكتروني، غرف المحادثة والمجموعات الإلكترونية .

ويستخدم الكثير من التنظيمات الإرهابية هذه المواقف الإلكترونية لشن الحرب النفسية ضد الدول المعادية وقواتها المسلحة، من خلال عرض افلام مرعبة للرهائن والاسرى أثناء إعدامهم، واغتيال العسكريين في الميدان على أيدي القناصين، أو إسقاط طائراتهم بالقذائف المحمولة على الأكشاف، أو نسف عرباتهم باستخدام القنابل المخفية على جانب الطرق أو على يد مفجرين انتحاريين.

وتسعى الرسائل الشفهية والمصورة تثبيط عزيمة العدو وتخيفه أو خلق شعور بالذنب والشك والأنشاق الداخلي، في الوقت الذي تبلغ فيه رسالة تهديد إلى الحكومات المختلفة ومواطنيها، ويحرز الإرهابيين قوتهم من رد الفعل على ما قد يثرونه من خوف لدى العدو.

ومن هنا فإن الإرهاب السيرياني قد شكل قاعدة للتغيير والتعبير ذلك مما آل إليه الإنترنت من تقسيم الرؤى المتطرفة التي تتبنى العنف أسلوباً ووسيلة، مستفيد الجمهور إلى فئات ومجموعات صغيرة، وأخذ هذا التنوع في تنمية ظاهرة التشتت الثقافي، بوصفه اعمالاً تستخدم إل فتوى ذكاء نيران الصراعات العنصرية وتنمية اتجاهات الكراهية لدى الكثير من الفئات المناهضة للفئات الأخرى، وفي مقابل تلك النظرة التفتيتية للمجتمعات، جاء ذلك العالم للترويج لرؤى عالمية، ففي حين تستغله الولايات المتحدة للترويج للرأسمالية والهيمنة، تستغله تنظيمات إرهابية للترويج للخلافة الإسلامية.

لقد قوض الإرهاب السيرياني من سلطة الدولة بنقل الحوادث الإرهابية إلى الرأي العام، بما يشكل وضغطاً على الحكومات بإجبارها على المشول للمطالب السياسية نفسي خطر التي تتبناها الجماعات الإرهابية وتهديداً لشرعية النظم

السياسية الحاكمة، وعمل ذلك على الحد من استخدام القوة في صنع القرار من جانب الدولة التي فرض انسحابها من قطاعات استراتيجية لصالح القطاع الخاص تحديات أمنية متزايدة.

وتطرح مسألة المواجهة الأمنية قضية حرية الرأي والتعبير عبر الإنترنت وارتباطها بالقيم الديمقراطية وكذلك مسألة الاستغلال السياسي للنظم الحاكمة لمواجهة معارضيتها بشكل الذي يعكس الفصل بين أمن النظام وأمن المجتمع، وفي مقابل تلك الجهود الغالبى مواقع الإنترنت، تزداد قدرة الإرهابيين على استخدام الفضاء الرقمي بشكل أكثر عمقا. (Grant, 2007)

وقد مثلت عملية التزاوج بين العالم والإرهاب في مجال استخدام العالم السلاح الجماهيري، أحدهما سلبي بحيث إنها قد تكون سبباً لنشر الرعب والخوف على المال من خلال تغطيتها غير الواعية للعمليات الإرهابية وآثارها محققة بذلك للإرهابيين هدفين مهمين هما:

الأول: هو إثارة الرأي العام ولفت انتباهه إلى وجود ظاهرة الإرهاب، إلا أن الإرهابي صاحب قضية يجب والاعتراف والاهتمام بها ومعالجتها.

الثاني: هو الحصول على الشرعية الدولية لما يطالب به الإرهابيون.

ويحرص الإرهابيون على تنفيذ عمليات مثيرة من حيث الأسلوب، أو حجم الخسائر، أو مكان وزمان وقوعها ليكون ذلك مدعاة لجذب الإعلاميين الباحثين دائماً وفقاً لطبيعة عملهم، عن الاختبارات المثيرة والمهمة بالنسبة لأكبر عدد ممكن من الجماهير.

أما الجانب الايجابي للسلاح فيتمثل في التغطية الواعية لقضايا الإرهابيين وعملياتهم، والرأي العام من تلك الأعمال الإجرامية، وفق أسلوب توعية يبرز بشاعة مرتكبيها وعداءهم للمجتمع، وسعيهم إلى التدمير والتخريب ونشر القلق في أوساط الافراد والمجتمعات والإرهاب كعنصر من عناصر القوة العسكرية والهجوم المسلح: ا ثالثةً كما هو الحال في أي حرب، فإن الجيوش المتصارعة تستهدف دوم أمور أساسية من أجل كسب المعركة، هي العناصر العسكرية، الاقتصادية و السياسية، أو بعبارة أخرى "اردة الخصم".

وفي عالم حروب المعلومات نجد العناصر بالتسميات الذاتية: مراكز القيادة والتحكم العسكرية، البنوك والمؤسسات المالية، مؤسسات المنافع كمؤسسات المياه والكهرباء، وذلك لاضعاع اردة الشعوب، وادارات دولة شبكة الإنترنت بشكل متعمد، فإن دولة أخرى قد تعتبر هذا الأمر عملً عدائياً عدائياً، وقد لا يكون الهدف هو تدمير الشبكة أو تعطيلها، كلي بحيث إنها تساعد حتى الطرف المعتدي في مراقبة المحادثات بين الاعداء أو نشر معلومات خاطئة الأمر الذي الذي يعتبر فرصة استخباراتية مذهلة.

أن استخدام الإنترنت في السيطرة على المعلومات يمكن أن يعود بفائدة تفوق الفائدة المطلوبة من تعطيل الشبكة نفسها أو تعر يضها للهجوم، خاصة عندما يخص الأمر الاستراتيجية العسكرية، العمل على إضعاف إرادة الجيوش، شن حرب نفسية و التحكم وفي المعلومات

وتعتبر هجمات شبكات الكمبيوتر، أو الحروب السيبرية جزءاً من عمليات المعلومات التي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة،

سواء على الجانب التكتيكي، الاستراتيجي، أو العملياتي ويتم استخدام الهجمات في أي وقت، سواء في وقت السلم أو الحرب أو الازمات، وتوجد طرق عديدة يمكن من خلالها تنفيذ الهجمات عبر الفضاء الإلكتروني، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات المهمة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة، وهناك أيضا سرقة المعلومات من أجهزة الخصم، ومن ثم إتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات، وبالطبع هناك استخدام الفيروسات والاساليب الإلكترونية، مثل هجمات الحرمان من الخدمات للتأثير على مواقع الخصم، مما يؤدي إلى التقليل من قدرة العدو على الاتصال وبطء قدرته على إتخاذ القرار تتضمن هجمات الكمبيوتر حدوث هجوم على خطوط الاتصالات، وتأتي تلك الهجمات من مسافة بعيدة عن مصدر الهجوم، من خلال الشبكات الدولية للمعلومات العابرة للحدود، موجات الراديو، أو الشبكات الدولية للاتصالات، بدون تدخل مادي، أو طبيعي في الاراضي الخاصة بدولة أخرى، أو القيام بغزوة تقليدية.

وعلى الرغم من الاستخدامات الحديثة لهجمات الفضاء الإلكتروني في الصراعات الحديثة، فإنه لم يتم إدماجها بشكل كامل في العقيدة العسكرية للجيش الحديثة، تمهيداً لبداية الأخذ بها بعين الاعتبار في سبيل الاستحواذ على القوة وامتلاكها من خلال تطوير أسلحة الفضاء الإلكتروني ليتم استخدامها في حروب المستقبل، بما ينطوي عليه تغيير المبادئ الخاصة بشن الحرب، ميدان الحرب، الطرق والوسائل الحربية المتاحة.

لقد ظهر الفضاء السيرياني كأحد مجالات الحرب، مثله في ذلك مثل الجو والفضاء الخارجي والأرض والبحر، وأصبح يستخدم كمجال عسكري وغير سلمي، وقد لا تؤدي الحرب في الفضاء الرقمي نأ إلى فرض نوع من السيطرة على مجرى الأحداث في العالم وفق إلى مأساة إلكترونية بالضرورة، ومصلحة من يشنها على جبهة واسعة النطاق من السهل الاحتفاء بها، كما أن آثار الهجوم قد لا تتساوى مع تكاليفه، فضلاً عن صعوبة تحديد هوية مصدر الهجوم الذي يصدر من جانب واحد، الأمر الذي يجبر ضحايا الهجوم على اتخاذ وضع الدفاع، مع عدم قدرتهم على شن هجوم مضاد، وفي حالة حدوثه، لعدم معرفة مصدر الهجوم يكون تأثيره محدود. (صليحي، 2019)

وتعتمد القدرة القتالية في الفضاء السيرياني على نظام التحكم والسيطرة، وقد أوجدت ملايين الأجهزة المثيرة للقوة، الكمبيوتر المنتشرة في كل مكان عالمياً افتراضياً نشأ نتيجة عملية الاتصالات، ل ذلك وسيطاً جديد بحيث يمكن للقراصنة دخول المجال الرقمي ومحاولة السيطرة على الأجهزة، فسادها وسرقة المعلومات أو تعطيلها، وذلك بعدما أصبحت المجتمعات والجيش الحديثة على أجهزة الحكم كبيراً مد اعتماد بيوتر، الأمر الذي يعرضها للخطر، فصار الإنترنت بهذا المضمون مرادفاً للاستخدام "الذكاء الاصطناعي". (توريه، 2011)

لقد ظهرت أسلحة سيريانية جديدة ومتعددة كالفيروسات، الهجمات الإلكترونية، الاختراقات القرصنة، سرقة المعلومات، التشويش، وتلاعب القنابل الإلكترونية دور كبيراً جداً في تنفيذ عدد من المهام الاستراتيجية، مثل تعطيل الاتصالات والتشويش عليها، التنصت على المكالمات، بث معلومات مضللة عبر

شبكات الحاسوب الآلي والهاتف، تقليد الاصوات، وخاصة أصوات القادة العسكريين، وعن طريق ذلك يمكن إصدار أوامر خطيرة، استهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات، مسح الذاكرة الخاصة بالأجهزة المعادية، منع تدفق الأموال وتغيير مسار الودائع، إيقاف محطات الكهرباء عن العمل، وقد صممت لذلك الهدف قبلة إلكترونية خاصة أطلق عليها اسم "bu49" تنطلق منها عدة قنابل في الجو تستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها الكامل. وبناء على ما سبق ذكره، يمكن يتصف الفضاء السبيرياني من حيث تعرضه لأمطار الحرب والصراع إلى صراع مرتفع الشدة وآخر مُنخفض الشدة.

وقد جاءت الحرب المنخفضة الشدة بصورة مستمرة ودائمة، وهي تعبر عن صراعات أعمق وأطول أمدا وترتبط بالصراعات ذات الطبيعة المعقدة والمتداخلة، وأصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بجميع أنواعها بين الفرقاء، ولا يمكن إحصاء الحالات التي تحتوي على هجمات إرهابية و معظمها يركز على جرامية، ولكن مراكز الطاقة، والبنى التحتية لنظم الاتصالات، وشركات الإنترنت، نظام مراقبة الملاحة الجوية، المصارف، مهام الجيش، وغيرها، ولا يزال يشهد مرشح حتم الصراع بكل أمطه عبر الفضاء الإلكتروني في بدايته، بيد أنه غير مسبوق في أساليب الصراع والرقابة والدفاع وطبيعة في غضون السنوات القليلة المقبلة تنو الأطراف، من باب أن ميدان المعركة والحرب هو الفضاء الإلكتروني.

ويرتبط هذا النوع من الصراع بميادين الحرب الإلكترونية وبأسلحة إلكترونية جديدة توازت مع مثيلتها التقليدية في نتائجها التدميرية، إن لم تكن قد تفوقت عليها، وفرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة، فالصراعات في

عصر المعلوماتية تتميز بأنها لا تنتهي حتى بانتهاء مظاهر الصراع المسلح وتمثل بيئة وسياقا إما للتطور نحو الحرب بشكل ساخن عبر تحريك الالة العسكرية، أو للتعبير عن غمط طبيعي وخالفات تدخل في سياق التنافس الذي يعد سمة أساسية من سمات المجتمع البشري أو جزءاً من عمل أجهزة الاستخبارات الدولية، أو التنافس بين الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

وهناك عدة أغمط تتعلق بالتهديدات السيبرانية، وتنقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أغمط رئيسية هي:

أ. هجمات الحرمان من الخدمة:

حيث يتم اطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على مُعالجتها والإستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضرراً للمستخدم النهائي، وهي تستعمل كثيراً ضد مواقع الإنترنت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

ب. إتلاف المعلومات أو تعديلها: ويقصد به الوصول إلى معلومات الضحية عبر شبكة الإنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية.

ت. التجسس على الشبكات: ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، والهدف منه الحصول

معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلباً على مهام الخصم.

ث. تدمير المعلومات: ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه "تهديد لسلامة المحتوى" ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك من يميز بين عدة أنواع من المخاطر والتهديدات السيبرانية والتي تتمثل فيما يلي:

1. التعرض لسرية الاتصالات التي تطال البريد الإلكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.
2. التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات، الجرائم العادية التي تستخدم الإنترنت، للسرقة والغش وسرقة الهويات والاعتداء على الملكية الفكرية وغيرها.
3. الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد أمن الأفراد والدول، كغسيل الأموال والإرهاب، كالتحديات الأمنية الخاصة بنظام الفدية، وهي أداة إجرامية انتشرت عبر الانترنت لعدة من الأفراد والإقتصادات، على المستوى الفردي سنوات، مستمرة في التطور وتشمل لها حيث التي تزال لا تزال حملات القرصنة بنظام الفدية، وتحقيق عائدات كبيرة للقرصنة ففي الإمارات وحدها، تم خسارة حوالي 1,1 مليار دولار أمريكي من أفراد المجتمع اتلانشطة الجريمة السيبرانية في عام 2017.

المبحث الثاني: الجريمة السيبرانية

الجريمة السيبرانية:

شهد العالم ثورة كبيرة في مجال تكنولوجيا الحسابات الآلية ومعالجة البيانات أطلق عليه مصطلح صناعة المعلوماتية، حيث ظهرت منافذ استثمارية جديدة تمثلت في مؤسسات وشركات ومشروعات فردية، منها ما يهتم بتصنيع الحسابات، ومنها ما هو موجه لاعداد البرامج فيها بصفة عامه، وأخرى تتولى إعداد الاطارات الفنية المختصة في تشغيلها.

ولعبت الثورة المعلوماتية بشكل كبير في تغيير العديد من المفاهيم القانونية خاصة في القانون الجنائي نظرا لظهور قيم حديثة ذات طبيعة خاصة، ومع قلة وجود النصوص القانونية الخاصة بتلك الجرائم "جرائم الحاسب الآلي"، هل يمكن الاستعانة دائما بالقواعد العامة في التجريم كمبدأ عام؟ وهل هي كافية للتصدي لأخطار التعدي على برامج الحاسوب والمعلومات التي يحتويها؟ أم لا بد من تدعيمها بقواعد تجرمية جديدة تتناسب والطبيعة الخاصة لبرامج الحاسوب؟ ويبقى السؤال الأهم: هل ثمة إتفاق على إصطلاح واحد بخصوص جرائم الكمبيوتر؟

وقد صنفت هذه الجريمة بأنها جريمة تقاوم التعريف " **resists definition** " لكثرة ما تناولته الكتابات عنها شرحا وتوضيحا؛ فمنهم من نظر اليها من خلال وسيلة إرتكابها ومنها من خلال موضوعها، ومنها من خلال توافر المعرفة بتقنية المعلومات ووجهات نظر مختلفة.

ولا تتحقق الحماية القانونية للنظم السيبرانية، وللموضوعات الناشئة عنها الا من خلال قواعد قانونية تجرم كل فعل يهدف الى الاعتداء ضد هذه النظم، او يهدف إلى

استخدامها كوسيلة لارتكاب إحدى الجرائم التقليدية، وهذا يتطلب تدخل القضاء لتوسيع نطاق النص الجنائي ليستوعب هذا النوع من الجرائم، وقد يتطلب تدخل التشريعات لسن قواعد قانونية خاصة بها، وهذا ما حدث في اغلب دول العالم . (دريس، 2013)

وتتطلب مواجهة المخاطر السيبرانية، إيجاد التعريف المناسب، الذي يحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر السيبرانية، كتلك المسببة والمؤذية، والتي تستتبع بالتالي، تحديد مسؤولية القائمين بها، كما تحديد السلوك الواجب اتباعه، والذي يعني عدم الالتزام به، امتناعا او اهمالا، ترتب مسؤولية هو الآخر. ويستدعي هذا الأمر بداية، تعريف الجريمة السيبرانية، التي تشكل الخطر الاساس الذي تجب مكافحته. والتعريف ضروري، لكي يتمكن اختصاصيو المعلومات، من تحديد الافعال التي لا بد من تلافي ارتكابها، وتلك التي لا بد من التبليغ عنها، كما يسمح للسلطات المعنية بالمكافحة، من التحرك على أساسها بدءا من اصدار مذكرات التفتيش والتحري، وصولا الى المصادرة والحجز وجمع الادلة. كذلك، يسمح تعريف الجريمة السيبرانية، للسلطات القضائية، بتعيين النصوص الملائمة، وإيجاد التفسيرات الصحيحة، وللسلطات السياسية، برسم خطوط التعاون مع البلدان الآخر، وان الصعوبة التي تنشأ عن ان بعض الأعمال الجرمية، في بلد ما، يمكن الا تكون كذلك، في بلد آخر، ما يستدعي، معالجة خاصة ومقاربة مشتركة، من البلدان المعنية، بالتعاون لمكافحة الجريمة السيبرانية، والحد من تأثيرها على الثقة والأمن، في المجال السيبراني. فتعريف الأعمال الجرمية، هو الخطوة الأولى، نحو مكافحتها، والسيطرة عليها.

وانسجاما، مع هذا المنطق، كما مع مبدأ " لا جريمة ولا عقاب دون نص" عمد العديد من البلدان، الى وضع نصوص قانونية، خاص، بهذا النوع الجديد من الجرائم، التي يمكنها ان تشمل مروحة واسعة من الأعمال غير الشرعية، كتلك التي تستخدم اجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة، او كهدف لها، بدءا من عمليات اختراق الأنظمة المعلوماتية وانظمة الاتصالات، وصولا الى الهجمات التي تعطل الخدمات. كذلك، تشمل الجريمة السيبرانية، فئة الجرائم التقليدية، التي تنفذ عبر المجال السيبراني. الا ان عدم وجود تعريف شامل، اضافة الى تنوع التعريفات الوطنية، والطبيعة العالمية، للمخاطر وللجريمة، يجعل من الافضل، ان ننطلق من التعريفات التي اعتمدتها، الهيئات والمنظمات الدولية المتخصصة، لايجاد المقاييس الخاصة بهذا التعريف، وذلك، بالرغم من كونها، تعريفات غير نهائية او غير محددة كفاية. ففي ورشة عمل متخصصة حول المسائل التي تثيرها الجرائم المتصلة بالشبكات، قسمت هذه الجرائم، الى مجموعتين، ضمنيت الأولى، حسب المدلول الاضيق، الذي يشير الى كل تصرف غير شرعي موجه بالوسائل الإلكترونية، نحو أمن أنظمة المعلومات، والبيانات التي تحويها، بينما ضمنيت المجموعة الثانية، حسب المدلول الاوسع، كل تصرف غير شرعي يرتكب بواسطة، الأنظمة المعلوماتية، او بطريقة متصلة بها، ويشمل جرائم كالحيازة غير المشروعة، او عرض الخدمات وتوزيع المعلومات، بواسطة أنظمة معلومات او شبكات معلومات.(الشهري 2001)

ساهم التقدم التكنولوجي والإنترنت في التطور المذهل لوسائل الاعلام والاتصال في العالم على جميع الاصعدة والمستويات، الأمر الذي أدى إلى إفراز نوع

جديد من الجرائم وهي ما اصطلح عليها بالجرائم السيبرانية، وقد بدت النصوص الجزائية التقليدية قاصرة عن مالحق بهذا النوع من الجرائم، ذلك أن التشريع وليد الحاجة، وبدأ المجتمع الدولي في تنظيم تشريعات لمواجهة هذا النوع الجديد من الجرائم الذي ظهر مصاحبا لاستخدام الحاسب الآلي، وإن ثمة تباين كبير بشأن المصطلحات المستخدمة للدلالة على هذه الظاهرة الإجرامية الناشئة في العالم الافتراضي.

ولم تتطرق التشريعات العربية إلى جرائم الحاسب الآلي إلا فيما ندر، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية حديثة النشأة، لان الاعتمادات على تطبيقات الحاسب الآلي فيها بدأ في نهاية العقد الاخير من القرن الماضي، على عكس البلدان الغربية التي إعتمدت الحاسب الآلي منذ عقدين من الزمن أو أكثر.

وتعرف الجريمة السيبرانية على انها فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الاموال المادية أو المعنوية، أو الاعتداء على خصوصية الافراد، أو هي عمل أو امتناع يأتيه الإنسان اضراراً بمكونات الحاسب الآلي وشبكات الاتصال الخاصة به ، من جهة اخرى هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، اما ضد الاموال كالتحويل الالكتروني، غير المشروع للاموال، او ضد الاشخاص كجريمة السب او القذف عبر الإنترنت. (دریس، 2013)

لقد خلف التطور التكنولوجي، وقد أخذت إن الإجرام السيبراني هو أحد النتائج السلبية التي هذه الظاهرة الإجرامية التي فرضت نفسها على المجتمع، حيزا كبيرا من

الدراسات من أجل تحديد مفهومها، حيث نجد أن العديد من الأعمال الأكاديمية حاولت وضع تعريف للجريمة المرتكبة عبر الإنترنت، هذه الأخيرة تعد من بين الجرائم التي تباينت تسمياتها عبر المراحل تقنية المعلومات، فقد أُصطلح على تسميتها في بادئ الزمنية لتطورها، والتي إرتبطت بتطور الأمر بإساءة استخدام الكمبيوتر، ثم جرائم إحتيال الحاسوب، فالجريمة السيبرانية بعدها جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، ثم جرائم التقنية العالية إلى جرائم الهاكرز فجرائم الإنترنت، وأخيراً جرائم السيبرانية. (مهمل ، 2018)

وتتطلب مواجهة المخاطر السيبرانية، إيجاد التعريف المناسب، الذي يحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر السيبرانية، كتلك المسببة والمؤذية، والتي تستتبع بالتالي، تحديد مسؤولية القائمين بها، كما تحدد السلوك الواجب اتباعه، والذي يعني عدم الالتزام به، امتناعاً او اهمالاً، ترتب مسؤولية عليه هو الآخر، ويستدعي هذا الأمر بداية، معرفة ماهية الجريمة السيبرانية، التي تشكل الخطر الاساس الذي تجب مكافحته، والتعريف ضروري، لكي يتمكن اختصاصيو المعلومات، من تحديد الافعال التي لا بد من تلافي ارتكابها، وتلك التي لا بد من التبليغ عنها، كما يسمح للسلطات المعنية بالمكافحة، من التحرك على أساسها بدءاً من اصدار مذكرات التفتيش والتحري، وصولاً الى المصادرة والحجز وجمع الأدلة. (الصحيفي، 2020)

كذلك، يمكن تعرف الجريمة السيبرانية، منقبل السلطات القضائية، بتعيين النصوص الملائمة، وايجاد التفسيرات الصحيحة، وللسلطات السياسية، برسم خطوط التعاون مع البلدان الآخر، وان الصعوبة التي تنشأ عن ان بعض الأعمال

الجرمية في بلد ما، يمكن الا تكون كذلك، في بلد آخر، ما يستدعي، معالجة خاصة ومقاربة مشتركة، من البلدان المعنية، بالتعاون لمكافحة الجريمة السيبرانية، والحد من تأثيرها على الثقة والأمن، في المجال السيبراني فتعريف الأعمال الجرمية، هو الخطوة الأولى، نحو مكافحتها، والسيطرة عليها.

وانسجاما، مع هذا المنطق، كما مع مبدأ "لا جريمة ولا عقاب دون نص" عمد العديد من البلدان، الى وضع نصوص قانونية، خاص، بهذا النوع الجديد من الجرائم، التي يمكنها ان تشمل مروحة واسعة من الأعمال غير الشرعية، كتلك التي تستخدم اجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة، او كهدف لها بدءا من عمليات اختراق الأنظمة المعلوماتية وانظمة الاتصالات، وصولا الى الهجمات التي تعطل الخدمات كذلك، تشمل الجريمة السيبرانية، فئة الجرائم التقليدية، التي تنفذ عبر المجال السيبراني. الا ان عدم وجود تعريف شامل، اضافة الى تنوع التعريفات الوطنية، والطبيعة العالمية، للمخاطر والجريمة، يجعل من الافضل، ان ننطلق من التعريفات التي اعتمدتها، الهيئات والمنظمات الدولية المتخصصة، لايجاد المقاييس الخاصة بهذا التعريف، وذلك، بالرغم من كونها، تعريفات غير نهائية او غير محددة كفاية، ففي ورشة عمل متخصصة حول المسائل التي تثيرها الجرائم المتصلة بالشبكات، قسمت هذه الجرائم، إلى مجموعتين، ضمنت الأولى، حسب المدلول الاضيق، الذي يشير الى كل تصرف غير شرعي موجه بالوسائل الإلكترونية، نحو أمن انظمة المعلومات، والبيانات التي تحويها، بينما ضمنت المجموعة الثانية، حسب المدلول الاوسع، كل تصرف غير شرعي يرتكب بواسطة، الأنظمة المعلوماتية، او بطريقة متصلة بها، ويشمل جرائم كالحيازة غير المشروعة، او عرض الخدمات وتوزيع المعلومات، بواسطة انظمة معلومات او شبكات معلومات.(الشهري 2001)

والجريمة السيبرانية هي جريمة تنطوي على استخدام أجهزة الكمبيوتر والإنترنت. ويمكن أن ترتكب ضد فرد أو مجموعة من الناس أو الحكومة أو المنظمات الخاصة. وعادة ما يقصد بها الإضرار بسمعة شخص ما، أو التسبب في ضرر بدني أو عقلي، أو الاستفادة منه، على سبيل المثال، الفوائد النقدية، ونشر الكراهية والإرهاب، وما إلى ذلك. وكما حدث في عام 1998، أرسلت مجموعة من مقاتلي التاميل، تعرف باسم عمور التاميل، أكثر من 800 رسالة إلكترونية إلى السفارات السريلانكية. وجاء في الرسائل "نحن عمور الإنترنت السود ونحن نفعل ذلك لتعطيل الاتصالات الخاصة بك." حددت سلطات الاستخبارات أنه أول هجوم معروف من قبل الإرهابيين ضد أنظمة الكمبيوتر في بلد ما. (Tripathi, 2019)

من جهتها، عمدت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، إلى إيراد ما تعتبره أعمالاً غير شرعية تحت عناوين تناولت، الجرائم ضد سرية الأنظمة والبيانات، وسلامتها، وتوفرها، والجرائم المتصلة بالأجهزة والجرائم الخاصة بالمحتوى، والجرائم الخاصة بالملكية الفكرية والحقوق المجاورة.

وتعد الجرائم السيبرانية من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مروراً بإصطلاح إحتيال الكمبيوتر، والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الإنترنت إلى آخر المصطلحات الجرائم السيبرانية. (الصحفي، 2020)

فمنهم من عرف الجرائم السيبرانية : بأنها "هي التي تتم بواسطة الكمبيوتر ،أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل، التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينهما.(الصحفي،2020)

ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفاً جديداً للجريمة السيبرانية، ففقهاء القانون لم يستقروا على تعريف واحد، فنحن لا نستنكر ذلك أبداً لأنه من الطبيعي جداً أن يكون هذا الاختلاف، وهذا التنوع في المفاهيم والآراء، وذلك يرجع لحدثة الجرائم السيبرانية، والاختلافات الثقافية والقوانين بين الدول ، وأيضاً خشية في أن يحصر المصطلح في نطاق ضيق أو محدود.(مهمل، 2018)

ويمكن اعتبار الأمن السيبراني مجموعة من المبادئ التوجيهية والإجراءات المقصودة والمطلوبة لمنع الجريمة السيبرانية، ولكن الأمن السيبراني لا يقتصر على ذلك فحسب. ويختلف نوعاً المشاكل اختلافاً كبيراً من حيث ما يحدث ومن هم الضحايا، فضلاً عن المجالات الأكاديمية التي تدرسهما. ولذلك، يجب النظر إلى الجريمتين، الأمن السيبراني والجرائم السيبرانية، على أنها قضيتان منفصلتان، مع ضمانات مختلفة مصممة لمعالجة مختلف قضايا الخصوصية والأمن لكل منهما. تحتاج جميع أنواع البيانات سواء كانت شخصية أو حكومية أو مؤسسية إلى أمان عالي، وبعض البيانات، التي تنتمي إلى نظام الدفاع الحكومي، والبحث العلمي والتطورات، والبنوك، والبحوث الدفاعية وتنظيم التنمية، وما إلى ذلك هي سرية للغاية، وحتى كمية صغيرة من الإهمال لهذه البيانات قد تسبب ضرراً كبيراً للأمة أو

المجتمع بأسره، وبالتالي، فإن مثل هذه البيانات تحتاج إلى الأمن على مستوى عال جدا. (Tripathi, 2019)

مراحل تطوّر الجريمة السيبرانية:

مرت الجرائم السيبرانية بتطوّر تاريخي بدأ من إختراع الحاسوب عام 1946، وإنشاء الشبكة العنكبوتية وصولاً إلى الثورة العالمية في الإتصالات والتكنولوجيا، وبحكم هذا التطور تطورت الجريمة بشكل عام والجريمة السيبرانية بشكل خاص ويمكن ملاحظة مراحل تطورها بمايلي:

المرحلة الأولى:

ارتبطت هذه المرحلة بظهور إستخدام الكمبيوتر وربطه بشبكة الإنترنت، وكان ذلك في الستينات إلى السبعينات من القرن الماضي، وتميزت هذه المرحلة بعدم الانتشار الواسع الاستخدام تم خلالها رصد عدد قليل من الجرائم بمعدل جريمة واحدة إلى ثلاث جرائم سنوياً، كما أن طريقة معالجة هذه الجرائم كانت في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة، والتدمير الذي يمس انظمة الكمبيوتر والتجسس. (سجواذ، 2015)

المرحلة الثانية:

شهد عقد الثمانينات إرتفاعا نسبيا في معدل الاجرائم السيبراني، حيث ظهر نوع جديد من الجرائم إرتبط بعمليات إقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر، ما تسبب في تدمير للملفات والبرامج، حيث شاع في هذه الفترة مصطلح الهاكرز، وهو مصطلح يطلق على مقتحمي النظم، وتعتبر قضية موريس الشهيرة من بين أهم القضايا المسجلة عبر الاف في فترة الثمانينات أين تم

نشر فيروس إلكتروني عرف بدودة موريس أجهزة الكمبيوتر من خلال الإنترنت.(سحواذ، 2015)

المرحلة الثالثة:

شهدت فترة التسعينات تطوراً هائلاً في مجال الإجرام السيبراني وتغيراً في نطاقها ومفهومها حيث أصبحت مواقع الإنترنت التسويقية الأنشطة أكثر عرضة للهجمات التي ظهرت بسببها أنماط جديدة من الجرائم، ففي سنة 1995 تم إختراق موقع البيت الأبيض الأمريكي، لتليها بعد ذلك العديد من الحوادث كحادثة شركة أوميغا فيروس وغيرها، و من أبرز الجرائم في هذه المرحلة قيام صبي بريطاني بإختراق شبكات الحواسيب العسكرية الأمريكية، و كشف عن أدق الاتصالات مما جعل المسؤولين الأمريكيين يصفونه بأنه أشد أنواع إختراق أمن شبكات الحاسوب خطورة هذا الاختراق على حالة الاستعداد العسكري.(مهمل، 2018)

المرحلة الرابعة:

وهي الفترة الممتدة من سنة 2000 إلى حد الان، حيث واكبها تطورات كثيرة ومتسارعة مع إرتفاع عدد مستخدمي الإنترنت ومعدلات الجرائم بالتبعية، وضخامة الخسائر المالية، وتواصل الجهود الدولية والوطنية لمواجهة هذه الجرائم، ففي عام 2002 بلغ عدد سكان العالم 28,6 مليار نسمة، وعدد مستخدمي الإنترنت 662 مليون مستخدم، ورغم ذلك لم تتفاعل حكومات دول العالم بالقدر المطلوب لتوفير الحماية اللازمة من الإجرام السيبراني، بالرغم من أنها صارت تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاع العام والخاص وعلى مستوى الافراد، وبعد الهجمات الإلكترونية الشهيرة على دولة إستونيا عام 2007، إنتبهت الكثير من

الدول لهذا الخطر الذي يدمر البنى التحتية للمعلومات وتقنية الاتصالات والشبكات، ويعطل كل المرافق الحيوية، فبدأت الدول التفكير بجدية في إعداد إستراتيجيات للأمن السيبراني. (بلعزوق، 2017)

المجرم السيبراني:

هو مجرم يتمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات وكسر الشفرات وكلمات المرور موظفا مهاراته تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات، كما أنهم في الغالب يتميزون بأنهم أفراد ذوي مكانة في المجتمع من أصحاب الوظائف الحيوية، سواء في القطاع الخاص أو في القطاع العام، وقد أطلق عليهم مصطلح ذوي الياقات البيضاء.

وقد ثبت من خلال الدراسات النفسية للمجرم السيبراني بأن ليس لديه أي شعور بعدم مشروعية الأفعال التي يمارسونها، وعدم استحقاقهم للعقاب، كما تغيب مشاعر الإحساس بالذنب، وذلك لربما عدم احتكاك الجاني المجرم بالمجني عليه مما يسهل المرور إلى الفعل الغير مشروع، وهم غالبا يخشون من اكتشافهم وافتضاح أمرهم.

أصناف المجرم السيبراني : (الصحفي، 2020)

1. الهواة : وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه .
2. القراصنة : ومنهم الهاكر : هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أو إثبات الذات، ومنهم الكراكر : وهم من يقومون بالتسلل إلى أنظمة المعالجة للاطلاع على المعلومات المخزنة إلحاق الضرر إما بالسرقة أو العبث بها .

3. المهووسون: ويكون المجرم في حالة الجنون الذي يهدف إلى تحطيم كل الأنظمة.

4. الجريمة المنظمة : فجهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا.

5. الحكومات الأجنبية: وذلك باستعمال أجهزة الحاسب في مجال الجاسوسية.

6. المتطرفون: وهم من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة.

أساليب المجرم السيبراني لارتكاب الجريمة السيبرانية

يستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة، و تتم عن طريق برنامجين الأول الخادم وهو بجهاز الضحية إذ ينفذ المهام الموكلة إليه، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، كما أنهم يستخدمون عدة برامج منها: (خالد،2020)

1. حصان طراودة: وهو عبارة عن برنامج صغير مختبئ ببرنامج أكبر، وتؤدي مهامها بشكل خفي في اطلاق الفيروسات والدودة التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام، وإرسال كلمات المرور السرية الخاصة بالهدف، ومن أنواعه القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطره.

2. فيروسات الكمبيوتر: وهي برامج صغيرة تستخدم لتعطيل شبكات الخدمات.

3. الديدان: وهي تكاثر عن طريق نسخ نفسها عن طريق الشبكات وهدفها الشبكات المالية مثل البورصات.

صور الجرائم السيبرانية، وهي كالآتي : (الزرفي، 2019)

أولاً: الاعتداء السيبراني على معطيات الحاسب الآلي : كاتلاف البيانات والمعلومات والبرامج والتلاعب بالمعلومات المخزنة داخل الحاسب.

ثانياً: الاعتداء السيبراني على حرمة الحياة الخاصة.

أ. يكون بالافشاء العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعة إصابته بمرض مخزي، أو عجز عن سداد ديونه أو نشر صورة البه .

ب. تشويه سمعة الشخص في نظر الجمهور، والتشهير به .

ت. الاستيلاء على بعض العناصر الشخصية كالاسم والصورة والبيانات الشخصية المتصلة بالحياة الخاصة.

ثالثاً: الاعتداء السيبراني على حقوق الملكية الفكرية : ويكون بالاعتداء على الاعلانات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرامج واعادة إنتاجها وصنعها دون ترخيص فهو اعتداء على الحقوق المالية والحقوق الأدبية.

رابعاً: الاستيلاء والنصب والاحتيال السيبراني: ويكون الاستيلاء إما لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

خامساً: الانتحال والتغوير السيبراني:

أ. انتحال شخصية فردية: بسبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم فتنتشر في شبكة الإنترنت الكثير من الاعلانات المشبوهة، والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات

اختيارية من الضحية، فهناك اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وهذا يتطلب الافصاح عن معلومات سرية، الأمر الذي يؤدي إلى استيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية، أو الاساءة إلى سمعة الضحية.

المحتوى غير المشروع

بالرغم من الارتباط الوثيق، بين نشر المحتوى غير المشروع والجرائم الإلكترونية، فاننا نرى ضرورة ابرازه كنقطة مستقلة فانطلاقا من مقولة ان ما هو غير مشروع على المستوى التقليدي، يبقى غير مشروع في الفضاء السيبراني، لا بد من النظر إلى المحتوى غير المشروع، كاحد المخاطر التي ترتبط مباشرة بأمن المجتمع والدولة، على السواء، ما جعل تنظيم وتشريع ما يمكن تداوله من معلومات، بواسطة اي من وسائل النشر، مسألة لصيقة بمهام الدولة الاساسية في حماية المجتمع، وحماية النظام القائم فيه، وبما ان مهمات الدولة لم تتغير، يبقى المحتوى غير المشروع، على الشبكة العالمية للمعلومات، وعلى وسائل النشر الإلكترونية كافة، في طليعة المسائل، التي لا بد من تأطيرها وتنظيمها، والمحتوى غير المشروع، يدعو الى التوقف عنده، على اكثر من مستوى، ونكتفي هنا، بالمستوى الاعلامي، ومستوى حماية الاطفال والشباب والثقافة التي ترتبط بهما. فممارسة النشر والاعلام الالكتروني، سواء عبر المواقع الاعلامية الرسمية، او عبر المدونات، والصفحات الشخصية على المواقع الاجتماعية، حولت مواقع عديدة، على الشبكة العالمية للمعلومات، الى منابر اعلامية، تطرح وتناقش، مختلف الآراء، والتوجهات والسياسات.

وعلى خط متصل، يطرح بث بعض أنواع المعلومات، والصور، والخدمات على الإنترنت، اشكالية حماية الشباب، والاطفال بشكل خاص، من المحتوى غير المشروع. ونذكر على سبيل المثال: عرض خدمات الدعارة، وبيع الكحول، والمواد الطبية غير المشروعة، والاستشارات الطبية غير المشروعة، والفلك، والميسر، والخطابات العنصرية، والمواقع الخاصة ببدع ومعتقدات تحرض على الانتحار أو على قتل الآخرين، هذا عدا، عن المواد الإباحية التي تستخدم الاطفال وتستغلهم. وإذا أضفنا، إلى كل ما تقدم، غياب تعريف عالمي، أو حتى اقليمي، لما يمكن اعتباره محتوى غير مشروع، بحسب ما تفرضه فعالية المكافحة في الفضاء السيبراني، ندرك، خطر هذا النقص وانعاساته العملية وعليه، فلا بد من العمل، للوصول، الى ايجاد أرضية مشتركة، ومبادئ عمل، تمكن من مكافحة المحتوى غير المشروع، وهنا يمكن للتقنيات أن تلعب دورا أساسيا، لاسيما من خلال تطوير برامج الترشيح والفلترية بناء على تعليمات محددة لهذا المحتوى غير المشروع، بحيث يمنع وصوله، على الأقل الى الاوطان التي تعتبره كذلك. وهنا أيضا، تبدو الحاجة ملحة، لمعالجة المدلول الواسع والمطاط، للمحتوى غير المشروع، في بعض التشريعات الوطنية، والتي يمكن معها للسلطة، أن تتصرف بالتفسير والقياس، الى درجة عالية، ما يؤشر الى امكانيات واسعة للاعتداء على حرية التعبير، وغيرها من الحريات المرتبطة بها، كالحق في الخصوصية، والحق في التعبير عن الرأي.

أسباب الجرائم السيبرانية:

للجرائم السيبرانية اسباب عدة منها ماييلي : (القحطاني، 2016)

1. الرغبة في جمع المعلومات وتعلمها.

2. الاستيلاء على المعلومات والاتجار فيها.

3. قهر النظام وإثبات التفوق على تطور وسائل التقنية.

4. الحاق الأذى بأشخاص أو جهات.

5. تحقيق أرباح ومكاسب مادية.

6. تهديد الأمن القومي والعسكري.

أنواع الجرائم السيبرانية

أولاً: جرائم التعدي على البيانات المعلوماتية:

تشمل الجرائم التي يكون موضوعها البيانات المعلوماتية، أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها. (بن داود، 2020)

ثانياً: جرائم التعدي على الأنظمة المعلوماتية:

تشمل جرائم الولوج غير المصرح إلى نظام معلوماتي أو المكوّن فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ويتمثل النظام المعلوماتي في مجموعة البرامج وأدوات معالجة وإدارة البيانات والمعلومات.

ثالثاً: إساءة استعمال الأجهزة أو البرامج المعلوماتية: (القحطاني، 2016)

تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً.

ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

رابعاً: الجرائم الواقعة على الأموال: (القحطاني، 2016)

- أ. جرم الاحتيال أو الغش بوسيلة معلوماتية.
- ب. جرم التزوير المعلوماتي.
- ت. جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية.
- ث. جرم أعمال التسويق والترويج غير المرغوب فيها.
- ج. جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المصرح لها.
- ح. جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها.

خامساً: جرائم الاستغلال الجنسي للقاصرات:

- هي الجرائم التي تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، والاتجار بهم وتشمل: (بن داود، 2019)
- (1) الرسومات أو الصور أو الكتابات أو الأفلام أو الإشارات.
 - (2) أعمال إباحية يشارك فيها القاصرون.
 - (3) تتعلق باستغلال القاصرين في المواد الإباحية.
 - (4) إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

سادسا: جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل جرام وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

سابعا: جرائم البطاقات المصرفية والنقود الإلكترونية:

تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

ثامنا: الجرائم التي تمس المعلومات الشخصية:

تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

تاسعا: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية: (بن داود، 2019)

1. جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية.
2. جرم تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية.
3. جرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.

4. جرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

عاشرا: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:

وتشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين وجرم ترويج المواد المخدرة.

الحادي عشر: الجرائم المعلوماتية ضد الدولة والسلامة العامة:

تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطل الدولة وسامتها وأمنها واستقرارها ونظامها القانوني، وهي: (القحطاني، 2016)

أ. جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية.

ب. جرائم الإغفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة.

وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو إخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية، وجرائم التحريض على القتل عبر الإنترنت أو أية وسيلة معلوماتية.

الثاني عشر: جرائم تشفير المعلومات:

تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، وأيضاً بيع أو تسويق أو تأجير وسائل تشفير ممنوعة. (القحطاني، 2016)

الفصل الثالث

الإرهاب والهجمات السيبرانية

المبحث الأول: الإرهاب السيبراني

يمكن لمصطلح "الإرهاب" أن يلمح إلى الاستخدام غير القانوني للسلطة أو الشراسة ضد الناس من أجل تهديد إدارة أو سكانها وجمعياتها التي قد تكون لإنجاز موقع سياسي أو خبيث تحول الإرهاب من الهيكل التقليدي إلى النوع الإلكتروني من الابتكار المدعوم بالإرهاب المعترف به على أنه إرهاب إلكتروني ويبقى قضايا حيوية للمجتمع الحالي، ليس فقط أن المعركة ضد الإرهاب متخلفة، فإن الاعتداءات الحالية على جرائم الإنترنت تنتهي بالقوة والمواجهة التدريبية، هذا الإرهاب هو استخدام الكلمة الإلكترونية لإرسال هجوم إلى الأسس الأساسية التي يعتمد عليها وجود الجمعيات والبلدان بالكامل بعد أن يؤدي ذلك إلى إغلاقه.

والفضاء السيبراني والإرهاب الإلكتروني، لا توجد تعريفات دقيقة بشأنهما، ففي مفهوم الفضاء السيبراني نجد حوالي 82 تعريفاً، يتناول معظمها مكوناته من أجهزة الكمبيوتر والوسائط التكنولوجية وشبكة الإنترنت، في حين أنه يتضمن أيضاً العنصر البشري أو المعنوي، وتشير كلمة Cyber أو Cybernetics إلى نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم محاكاة الآلات لها، وبالتالي فالمجال دراسة الاتصال والتحكم الآلي في النظم العصبية

للكائنات الحية ،والأمن السيبري يتضمن كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات، وتعرف كليات الحرب الأمريكية الإرهاب السيبراني، أو كما تسميه "هجمات الشبكات الكمبيوترية"، انطلاقاً من تصنيفه تحت بند "العمليات الإلكترونية"، وهو يندرج في إطار الحرب الرقمية، وعرف من خلال الاجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها، والإرهاب الرقمي يستهدف أمن العمليات، العمليات النفسية، الخداع العسكري الهجمات الفيزيائية، ومهاجمة شبكات الكمبيوتر، ولا يوجد إجماع حول تعريف الإرهاب السيبراني، لكنه يشير عموماً إلى شكل جديد من أشكال الإرهاب، ويندرج في إطار الجرائم الإلكترونية، وقد اخذ تسميته من استخدام وسائل، ووسائط التكنولوجيا المعلوماتية والاتصالية في تنفيذ أعمال إرهابية تتجاوز تداعيات الأبعاد المحلية والوطنية لتؤثر بشكل كبير على الأمن الدولي، ويتضمن الإرهاب الإلكتروني أو الرقمي بهذا المعنى أعمال اختراق المواقع وأنظمة المعلومات، القرصنة، ونشر الرعب وأشكال التهديد الموجهة نحو الافراد أو الدول، استقطاب الافراد للانخراط في التنظيمات الإرهابية. (حكيم،2018)

أما عن مكونات الإرهاب السيبراني فهناك عدد قليل من الهجمات والإرهاب السيبراني لديها عدد قليل من الأجزاء التي تم تمييزها من قبل العديد من الباحثين الاصدين في شبكة الاستكشاف في نموذجهم الافتراضي الاعتراف بالأقسام الخمسة التي "الإرهاب السيبراني" وتصنيفهم؛ الهدف من العنف والإلهام والتفاني نحو المهمة التي يتعين إنجازها عندما يقع مثل هذا الحادث، والأثر، وتستخدم الأدوات

لإرسال مثل هذا الاعتداء والهجوم، وهي المنطقة التي هي الطبيعة تماماً كما استراتيجية للنشاط. ويمكن أن نعرف بثقة من خلال معرفة ملامح الأنشطة التي تدفع أعمال الجناة القضية الحرجة في "الإرهاب السيبراني" هو الدافع لاستكمال مثل هذا العمل على شبكة الإنترنت، أن النتائج في وحشية الأضرار التي لحقت بالناس وممتلكاتهم، والإرهابيون مستمرين في الاتجاه السعودي لعالم الإنترنت مع حافز قوي كالمرحلة التي يمكن استخدامه والابتكار في استخدام المعلومات والمراسلات، ويمكن للإرهابي تقديم المزيد من الأضرار الجديرة بالملاحظة أو فرض شروط مزعجة على الجمهور بسبب انقطاع الإدارات اللازمة، وأن إرهابي الفضاء الإلكتروني" يسبب المزيد من الضرر والدمار من قبل الفضاء الإلكتروني كما فعلت الاستراتيجية التقليدية للإرهاب. (KALAKUNTALA & others, 2019)

العوامل التي تحفز الإرهاب السيبراني:

هناك عدد من العوامل المُحفزة للإرهاب السيبراني هي الآتية:

(KALAKUNTALA & others, 2019)

أ. الطبيعة الداعمة للمواقع الإلكترونية.

ينظر إلى الإنترنت على أنه وسيلة هائلة بشكل استثنائي، ويمكن أن ترسم في الوقت نفسه النظر في الاهتمام المشروع لبعض الأفراد للانضمام إلى مجموعة من الاهتمامات، ويفضل الإرهابي الإلكتروني استخدام الموقع نظراً لطبيعته القوية من حيث أنه يمكن أن يحيل رسالة إلى عدد كبير من الأفراد داخل طرفة عين؛ يعتبرونها مرحلة أي شيء ولكن من الصعب اختيار الأفراد استيعابها، عدم الكشف عن الهوية.

ب. طبيعة الإنترنت:

يعتبر عدم الكشف عن الهوية هو العنصر المحوري الذي يميل كل مذنّب الشر نحو الهدف الذي لا يمكن التعرف على شخصيتهم بعد اللعب بها فعل شيطاني، والإنترنت هو مجال محمي تماما كما إخفاء المرحلة للإرهابي لأنها يمكن أن تبقى غير معروفة بحيث لا يمكن أن تكون معروفة شخصيتهم.

ج. القرصنة:

ان المصطلح العام لجميع أنواع الوصول غير المعتمد إلى أي شبكة " نظام كمبيوتر " وتنظيم القرصنة التي يمكن أن تحدث في أي هيكل كل الأشياء التي تقاس على انها "القتل السيرياني" والعديد من هؤلاء القرصنة يمكنهم الاستفادة من "القوة الغاشمة" الذي هو مزيج من كل حرف واحد يمكن تخيلها تماما كما الأرقام والصور حتى يحصلوا على كلمة المرور.

هـ فيروسات الكمبيوتر:

توجد هذه الفيروسات مُتَنَاطرة هنا وهناك على نظام في غيرها للقيام بتمارين مؤذية، وقد تكون هذه ملئ كعامل إداري، إنشاء معلومات أو حتى تقسيم النظام.

و. شم كلمة السر:

قد تستخدم واحدة من هذه التقنيات مثل شم كلمة السر والإجراءات اللازمة لاستكمال "الهجوم السيرياني" على مختلف البلدان والعديد من المنظمات الكبرى لرؤية سقوطها، والسيطرة على أنظمتها، الشم لكلمة المرور هو البرمجة التي تستخدم لتنظيم الشاشة وفي الوقت نفسه التقاط كل كلمات المرور التي تعتبر موصل للنظام.

عواقب الإرهاب السيبراني:

الإرهاب السيبراني هو نوع أصلي من الخطر السيبراني، والهجوم الذي له العديد من النتائج المرتبطة به عندما يدفع ضد أي بلد أو روابط، وتعرف بعض عواقب الإرهاب السيبراني على النحو التالي: (KALAKUNTLA & others , 2019)

- قواعد البيانات:

يمكن للإرهاب السيبراني أن يبيد أمانة المعلومات بهدف أنه لا يمكن الوثوق بالمعلومات مرة أخرى، مما يؤدي إلى سحق تصنيفها على أنه تطفل على إمكانية الوصول إليها، وقد أدى ارتفاع معدل هذا الإرهاب السيبراني في التعدي على الجمعيات ومعلومات البلد إلى الكثير من الصعوبات التي نتجت عن فقدان الحيوية والمعلومات الهامة التي يصعب عادة استردادها.

- الهجوم على المؤسسات:

يمكن أن يؤدي الإرهاب الإلكتروني إلى خسارة المؤسسات مليارات الدولارات في منطقة المنظمات، ويمكن ترتيب البيانات من البنك ويمكن أن تتعرض للهجوم أو الإختراق من خلال الإرهابيين الذين سيدفعون للوصول غير المعتمد إلى مثل هذا التوازن المالي وجعلها تفقد الملايين العملاقة من الدولارات التي يمكن أن تخلق مثل هذا البنك للحفاظ على تشغيل في الإفلاس.

- خسائر في الأرواح:

وقد ضمن الإرهاب السيبراني فقدان العديد من الأرواح، وفي الوقت نفسه جعل العديد من المنازل في حالة من المشكلة التي تأتي في بعض الأحيان على وشك الإصابة العقلية للمتأثرين.

إن "الإرهاب السيبراني" يمكن أن يؤدي بطريقة أو بأخرى إلى إرتفاع عدد القتلى بنفس القدر الذي يسبب أضراراً جسيمة، وقد أظهرت في هجومات على استخدام أجهزة الكمبيوتر الشخصية، والشبكات فضلاً عن الهجمات التي لديها تأتي حول أنواع مختلفة من الانفجارات مع عدد قليل من حوادث .

– فقدان ثقة المستهلك:

إن تطوير المنظمات ودعمها يعتمد على الثقة التي لدى المستهلك، كما الثقة يمكن أن نرى الأدوات التي تحصن الارتباط واليقين بين المنظمات والعملاء.

متى يصنف الإرهاب بأنه سيبراني؟

يمكن لشخص ينتمي إلى منظمة إرهابية تنفيذ جميع الأنشطة التي تمت مناقشتها أعلاه، ولكن لكي يتم تصنيفها على أنها سلوك إرهابي يجب أن تكون بنية أو هيكل الإرهاب ومبدأ الضرر وعناصره موجودة، علاوة على ذلك، بالنسبة للإرهاب السيبراني، يجب تنفيذ السلوك الإرهابي "داخل" أو "من خلال" الفضاء الإلكتروني.

وبالتالي، ليست كل جرائم الكمبيوتر (بالمعنى الواسع أو الدقيق) التي يرتكبها "إرهابي" تشكل إرهاباً أو إرهاباً إلكترونياً. فلا يمكن وصف جميع الجرائم الإلكترونية أو الجرائم العامة التي يرتكبها شخص ينتمي إلى منظمة إرهابية بأنها إرهابية أو إرهاب إلكترونياً. كما لا يكون الإرهاب سيبرانياً عندما يرتكب شخص ينتمي إلى منظمة إرهابية عملاً إرهابياً باستخدام تقنيات أخرى غير شبكات الكمبيوتر.

أي أنه من أجل وجود الإرهاب السيبراني، يجب ارتكاب السلوك الإرهابي في الفضاء الإلكتروني. ولتنفيذ الأنشطة الإرهابية في الفضاء الإلكتروني، من الضروري

أن يكون للسلوك المنفذ في ،او من خلال الفضاء الإلكتروني ،هيكل ومبدأ ضرر والعناصر التي تسمح بتصنيفه على هذا النحو". كما يجب أن تكون جميع هذه المتطلبات (الهيكل ومبدأ الضرر والعناصر) حاضرة بشكل مشترك، وإلا فلا يمكن اعتبار السلوك المعني إرهاباً إلكترونياً؛ وبهذا فإن عناصر الإرهاب السيبراني الحقيقية هي: (الشرقاوي،2021)

أ. من حيث الهيكل : فإن الإرهاب الإلكتروني هو دائماً جريمة منظمة، على عكس الجرائم الفردية السيبرانية، فعلى الرغم من وجود وجهات نظر لبعض الأفراد يؤمنون بالإرهاب الذي ينفذه شخص واحد، وبالتالي، يمكنهم أيضاً قبول الإرهاب السيبراني الفردي، فإن الخطر المحدد الذي ينطوي عليه الإرهاب السيبراني يكمن في وجود جماعة منظمة تعمل بشكل منهجي لارتكاب عدد غير محدد من الجرائم، ولا يوجد مثل هذا الخطر في حالة عمل فرد أو مجموعة خاصة بمفردهم، وبالتالي فالحديث عن رابطة إرهابية إلكترونية إجرامية، يجب أن يكون هناك كما هو الحال مع الإرهاب التقليدي: عددًا محددًا من الأعضاء، مع إمكانية الوصول إلى الموارد والتمويل، بالإضافة إلى القدرة على التخطيط المستدام للعمليات وتنفيذها بمرور الوقت؛ فالإرهاب السيبراني يعتمد على الكثافة التنظيمية التي تتطلب وجود هيكل من الأشخاص لاتخاذ القرارات الجماعية، وللتنسيق والاستمرار مع مرور الوقت.

ب. من حيث مبدأ الضرر: لا يهاجم الإرهاب السيبراني المصالح الفردية بشكل مباشر، أي تلك التي تخص أو تخدم شخصاً معيناً أو مجموعة معينة من الأشخاص، فعلى العكس من ذلك، يؤثر الإرهاب السيبراني بشكل مباشر على

مصلحة جماعية مملوكة لعامة الناس أو تخدمهم. كما هو الحال في الإرهاب، فإن المصلحة الجماعية التي يهاجمها الإرهاب السبيرياني بشكل مباشر هي المصالح المؤسسية أو الحكومية أو الوطنية. وحتى لو كان الإرهاب الإلكتروني يضر أو يهدد المصالح الفردية مثل حياة الآخرين أو صحتهم، فإن هذا التأثير غير المباشر ليس هدفه النهائي، بل الهدف هو هجوم مباشر على النظام الدستوري الديمقراطي.

ت. من حيث العناصر الموجودة: يتألف الإرهاب السبيرياني من عنصر غائي وعنصر أدائي؛ فيما يتعلق بالعنصر الغائي، يجب ارتكاب الإرهاب السبيرياني بهدف تغيير النظام الدستوري أو إسقاط الحكومة المنتخبة شرعياً؛ لأن بالتبعية سيكون للجماعة الإرهابية الإلكترونية دائماً أجندة سياسية، أما فيما يتعلق بالعنصر الأدائي، يجب تنفيذ أعمال الإرهاب السبيرياني بطريقة مناسبة لبث الرعب في أذهان الناس مما يؤسس للاعتقاد بأن أي شخص في أي مكان يمكن أن يكون ضحية للإرهاب السبيرياني.

ولفهم سلسلة التحول من نطاق القرصنة إلى الوصول لعمليات الإرهاب السبيرياني؛ فإنه يندرج ضمن النموذج الأصلي "للقرصنة" والذي يبدأ في تنفيذ إجراءات متصاعدة الشدة: أولاً عن طريق إتلاف بيانات المستخدمين الفعليين، ثم تخريب المعلومات المخزنة بواسطة شركة كبيرة أو كيان حكومي كبير، وأخيراً توجيه هجوم ضد SCADA (التحكم الإشرافي واكتساب البيانات) أو البنية التحتية الحيوية من خلال استخدام التكنولوجيا، مع ملاحظة أنه عند مهاجمة الـ SCADA أو البنية التحتية الحيوية من خلال استخدام التكنولوجيا فإننا بذلك نخرج من نطاق

مجرد القرصنة وندخل في الإرهاب السيبراني، طالما أن جميع المتطلبات (الهيكل، مبدأ الضرر، العناصر) موجودة والتي تشكل إرهاباً فعلياً؛ ولهذا يمكن القول إن الإرهاب الإلكتروني هو دائماً خطوة واحدة وراء القرصنة.

وبهذا، فإن الإرهاب السيبراني ليس مجرد التلاعب بالبيانات أو البرامج التي تتسبب في خسارة عدد كبير من الأشخاص لمبالغ كبيرة من المال عبر الإنترنت، ما لم تستلزم هذه الخسارة دماراً اقتصادياً وما يترتب على ذلك من تأثير على حياة أو صحة ضحاياها.

آثار الإرهاب السيبراني من منظور علم النفس السياسي

للإرهاب السيبراني آثار عدة من وجهة نظر علم النفس تتمثل فيما يلي:
(الشرقاوي، 2021)

1. الآثار النفسية للإرهاب السيبراني : إن التعرض للإرهاب يقوض إحساس الفرد بالأمان، ويعزز نظرة عالمية مهددة ويزيد الدعم للسياسات المتشددة، ويسبب تحولاً مميّناً في قضايا الأمن والخصوصية ويؤدي إلى زيادة مطالب الحكومات باتخاذ إجراءات قوية من خلال العمل العسكري ضد الجماعات الإرهابية.

في حين أن افتقار الجمهور إلى التطور التقني وعدم الإلمام بالتعامل مع الفضاء الإلكتروني يؤدي إلى إثارة مشاعر الرعب وعدم اليقين وتضاعف إدراك التهديد، وهذه الظاهرة تشبه "العجز المكتسب" وهي عملية تعزز اللامبالاة لأن الناس يشعرون أنهم لا يستطيعون فهم الهجمات الإلكترونية أو الدفاع عنها.

ذلك علاوة على أن سرعة الإنترنت والحاجة اللاحقة لاتخاذ قرارات فورية في سياق الصراع السيبراني يمكن أن تزيد من التوتر، وتقلل التركيز وتعرض صنع القرار

للخطر. وأيضًا هناك نوع آخر من الإرهاب السيرياني قد يؤثر على النتائج العاطفية وهو تصويره الفريد في وسائل الإعلام، لأن تصوير وسائل الإعلام للإرهاب السيرياني بوصفه تهديدًا وجوديًا، أو أنه "قصة هلاك سيرياني"، يزيد من إدراك التهديد والاستجابة العاطفية إلى حد كبير.

فالتعرض للإرهاب السيرياني يثير القلق لأن الأعمال الإرهابية يُنظر إليها على أنها غير متوقعة وعشوائية ويصعب مواجهتها أو تجنبها، وبذلك يرتبط القلق بشعور من عدم اليقين وعدم السيطرة، مما يزيد من النفور من المخاطرة ويزيد من الدعم للإجراءات منخفضة المخاطر، وعلى النقيض من ذلك، ينشأ الغضب من الرغبة في تصحيح الظلم المتصور وبالتالي يرتبط بنتائج سياسية أكثر عدوانية.

2. أما عن الآثار السياسية للإرهاب السيرياني: فبالنظر إلى الإرهاب التقليدي كقوة إرشادية وفحص النتائج السياسية التي تتراوح من الأيديولوجية السياسية والمشاركة السياسية إلى التطرف ودعم العنف، وجد أن منطق الإرهاب الملتوي يستند إلى إثارة الشعور بالخوف والضعف بين السكان وتقويض الثقة في الحكومة، كما يستند على مواقف السياسة الخارجية بشكل عام، مع التركيز بشكل خاص على دعم الانتقام العسكري: (الشرقاوي، 2021)

أ. فمن حيث الإرهاب السيرياني والثقة العامة: فتصميم هذه الهجمات تكون بهدف زعزعة ثقة المجتمع في قدرة الحكومة على العمل والدفاع ضد الهجمات المستقبلية؛ وتعرف الثقة العامة على أنها التقييم الذاتي لقدرة الحكومات والقادة والمؤسسات الأمنية على منع الهجمات والحفاظ على دولة فاعلة، ولقد بحث علماء النفس السياسيون هذا الأمر ووجدوا أنه على عكس الحدس والإدراك

المتوقع، تستنتج غالبية الدراسات أن التعرض للإرهاب يزيد من الدعم العام للسياسات الحكومية والثقة العامة في المؤسسات الحكومية، وهي حقيقة لا ترتبط بالضرورة بمعالجة عقلانية لكفاءة الحكومة، في مواجهة التهديد المرعب، ولكن بسبب الحاجة إلى الأمن النفسي بسبب بيئة الخوف وعدم اليقين والغضب ويلعب علم النفس السياسي دوراً واضحاً في هذه الظروف لأنه في " حالات الصراع الدولي المفاجئ يصبح التقييم العاطفي وشدته، لا سيما مشاعر الغضب أو القلق، الأسس الأساسية لتقييم الحكومة وكذلك، يمتلك الإرهاب السيرياني صفات تميل إلى التأثير على الثقة على وجه التحديد، ومن أهم هذه المشاكل معضلة الإسناد، أو نوعية الغموض الذي يحيط بتحديد هوية مرتكبي الجرائم الإلكترونية، إذ تعمل صعوبة الإسناد هذه في اتجاهات متعددة ويمكن أن يؤدي عدم وجود معرفة بهوية المهاجم إلى زيادة إدراك المخاطر بسبب المعرفة المطلقة التي غالباً ما ترتبط بالعاملين عبر الإنترنت.

ب. ومن حيث الإرهاب السيرياني ومواقف السياسة الخارجية: فمن النتائج السياسية الرئيسية ذات الأهمية التي ترتبط غالباً بالتعرض للإرهاب والعنف السياسي مواقف السياسة الخارجية بشكل عام ودعم الضربات الانتقامية بشكل خاص، فالتعرض للعنف يؤدي إلى ضائقة نفسية وإدراك شديد للتهديد وتبني مواقف سياسية متشددة فيما يتعلق بالإرهاب السيرياني، والتعرض للهجمات الإلكترونية يؤدي إلى مطالب عامة بردود عدوانية وتصعيدية؛ أما الإرهاب السيرياني فهو شديد بما يكفي لتوليد مشاعر سلبية كبيرة بمستويات مكافئة لتلك الناتجة عن أعمال الإرهاب التقليدية، وثانيًا، أن هذا التعرض مرتبط ارتباطاً مباشراً بتبني

المواقف السياسية العسكرية والمطالبة بالانتقام الجسدي، وثالثاً أن المتغيرات
العاطفية المتداخلة كانت مماثلة لتلك التي أثارها الإرهاب التقليدي (أي
إدراك التهديد والقلق والغضب).

المبحث الثاني: الهجمات السيبرانية

لقد تعددت التعريفات التي تناولت مُصطلح الهجمات السيبرانية على ضوء الإجهادات الفقهية والممارسات العملية الدولية، فالهجمات السيبرانية مُصطلح تم استخدامه من قبل فئات عديدة من الاشخاص للإشارة، إلى أشياء مُختلفة، كالإشارة إلى وسائل القتال وأساليبه التي تتألف من عمليات في الفضاء الإلكتروني، والتي يمكن أن ترتقي إلى مستوى النزاع المُسلح، او انها قد تجرى في سياقه، ضمن المعنى المقصود في القانون الدولي الإنساني، ويمكن وصف الفضاء السيبراني الذي تجري فيه الهجمات السيبرانية بأنه عالم افتراضي مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نُظم الكمبيوتر وشبكات الإنترنت والمخزون الهائل من المعلومات والبيانات، حيث يتم الاتصال بشبكات الإنترنت عبر الحواسيب أو الهواتف او غيرها دون التقيد بالحدود الجغرافية، لذلك فإن الهجمات السيبرانية في هذا الاتجاه يمكن وصفها بأنها عبارة عن تصرف واقعي يدور في عالم قائم على استخدام بيانات رقمية ووسائل اتصال تعمل إلكترونياً، ومن ثم تطور هذا المفهوم، إلى ان أصبح يستخدم بشكل واسع، ويقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة جراء اختراق مواقع الكترونية ؛ عادة ما تقوم بوظائف تصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية، والمطارات ووسائل النقل الإخرى . (العيسى وعناب، 2018)

وقد عرفت الهجمات السيبرانية بأنها وسيلة قتالية من خلال استخدامها بذاتها للتسلل إلى أنظمة إلكترونية مُعدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية، أو السدود، أو وسائل النقل كالمطارات، بهدف

تطويعها والسيطرة عليها لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات غير صحيحة لاجهزة التحكم والحماية الإلكترونية، الا ان هذا الاتجاه تم توجيه النقد له، من منطلق ان هناك اتجاه رأى تصنيف الهجمات السيبرانية كونها وسيلة قتالية قد لا يكون صائباً لان الهجمات السيبرانية تفتقد للطاقة الحركية التي تعد أهم صفة تعترف بها الأسلحة التقليدية، لذلك فإنه من غير الممكن تحسس ومعرفة الهجوم السيبراني على نحو مادي، اضافة إلى أن وسيلة الهجمات السيبرانية لا تحوي مواد متفجرة، ولا يمكن ان يتم عجزها كوسيلة قتالية .
(العيسى وعناب، 2018)

وعرفت الهجمات السيبرانية ايضاً بأنها الذراع الرابع للجيش الحديثة إلى جانب القوات الجوية والبرية والبحرية، خاصة أن عصر الإنترنت الذي شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي ،وهناك من يرى أن الهجمات السيبرانية تمثل البُعد الخامل للحرب، وفي هذا الجانب تم تعريف الهجمات السيبرانية بأنها: "مجموعة من الاجراءات التي تتخذها الدولة للهجوم على نظم المعلومات العادية بهدف التأثير والضرار بها، وفي الوقت الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة، الا انه هناك من أشار إلى أن المقصود بها هو: "هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص الدخول إليها من أجل تعطيل البيانات المتوفرة فيها الاستحواذ، او الاتلاق عليها، وهي عبارة عن (سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى) .

ويمكن القول ان الهجمات السيبرانية: هي أي تصرف، سواء أكان دفاعياً أم هجوماً، يتوقع منه، وعلى نحو معقول، في التسبب بإصابة شخص، أو قتله، أو إلحاق

أضرار مادية، أو دمار بالهدف المدمر، إذ يعد هذا التعريف الاقرب والاشمل لمفهوم الهجمات السيبرانية. (الفتلاوي، 2016)

وتعريف الهجمات السيبرانية ايضاً من خلال الأمن القومي، وظهرت المستجدات العديدة في مجال تكنولوجيا الحرب بأن السيبرانية تعد تحدياً للمفاهيم السائدة حول الأمن القومي، وهذا يربط ايلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهمية قصوى لا سيما في مجالات الطاقة والاتصالات، والحوسبة، والمياه والمواصلات والاقتصاد في القطاعين المدني والأمني. وبناء عليه، ينبغي إجراء التعديلات اللازمة في مفهوم الأمن القومي؛ بهدف الرد على التهديدات المستجدة الناتجة عن الهجمات السيبرانية، فالتصدي للتهديد المستجد الناجم عن تطور تكنولوجيا الحرب السيبرانية يتلائم مع عقيدة الأمن القومي ألي دولة في الوقت الحاضر في الامكان بواسطة أدوات سيبرانية، والتي تتطلب قوة مادية كبيرة ولكنها تتطلب إعداد وتطويراً لمهارات القوة البشرية، وتنفيذ أنشطة تساهم في تعاضد قوة الردع للدولة، وترسخ مكانتها على الساحة الدولية. (الفتلاوي، 2016)

وهناك ركائز ثلاث لمفهوم الأمن القومي اللاتقليدي صالحة للتهديد السيبراني، وهي الآتي:

أولاً: الردع :

يمكن لأي دولة من ردع إن القدرات السيبرانية المتطورة، أعدائها فقيماً كان من السهل تقييم قدرات الدول وقوتها، لكن عبر مضي القرون، وازدهار التكنولوجيا وتطورها، تغيرت مصادر القوة و شكل الردع وأصبحت القوة الإلكترونية من أهم أدوات بعض الردع التي تستخدمها الدول في التنافل والتصارع مع بعضها على سبيل

المثال إن التغطية العالمية الواسعة التي حظي بها فيرول "ستاكسنت"؛ خدم لتخريب أنظمة الكمبيوتر التي أصبحت تتحكم بمرافق تخصيص اليورانيوم في إيران المنسوب إلى الولايات المتحدة واسرائيل، والذي شكل قفزة نوعية في كل ما يتعلق بالقدرة المتحدة، والهجومية السيبرانية للدول ونفوذها وقوتها .

ثانياً: الإنذار المبكر:

إن القدرات السيبرانية الهائلة للدولة ستتمكنها من جمع معلومات كثيرة عن أعدائها، وفي الوقت ذاته ستمنع هولاء من الوصول إلى قاعدة بياناتها وهذا يشكل بالنسبة للدولة إنذار.

ثالثاً : الحسم:

فالدول الرائدة في العالم من حيث قدراتها السيبرانية تكون متفوقة في المعركة من خلال ؛ استخدام أدوات سيبرانية متقدمة بهدف حسم المعركة، فالواضح اليوم أن التفوق السيبراني المتكامل مع قدرات حركية متقدمة، أصبح من شأنه أن يحسم المعارك .

نشأة الهجمات السيبرانية

ترتبط الهجمات السيبرانية مباشرة بحدثين مهمين: (الفتلاوي،2016)

الأول: استحداث أجهزة الكمبيوتر في مُنتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توجت بتطوير وحدة المعالجة المركزية، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز

الكمبيوتر، أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية للأفراد.

الثاني: ظهور الشبكة العنكبوتية (الإنترنت) والذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل من البيانات المرسلة عبر الأثير، وفي سياق متصل، يصف البعض أن نشوء الثورة المعلوماتية الحالية، هو بمثابة الجيل الثالث للثورات التقنية التي غيرت في أسلوب الحياة وإمكانيات البشرية، وبعبارة أخرى الثورتان الزراعية والصناعية، وأخيراً الثورة المعلوماتية.

لقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري، وذلك حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة في مطلع التسعينيات من القرن المنصرم السيرياني سباق التسلح أو، (Sommer & Brown, Cyber Cold War, 2011).

وفي بادئ الأمر لم يكن للهجمات السيبرانية صدى على المستوى الدولي، إذ نشأت الجريمة السيبرانية أولاً على هيئة جرائم طالت المؤسسات المالية والمصرفية، فضلاً عن الشركات المتخصصة ببرمجة نظم الاتصالات، وقد دأبت الدول على اتخاذ التدابير التشريعية لتجريم الأفعال وتحدي العقوبات.

وفيما يخص الدول واستخدامها للتكنولوجيا المتقدمة لأهداف عسكرية، فعادةً ما تلجأ إليها لأجل تحقيق مكاسب محددة، في أقل تقدير للهيمنة على واقع النزاع المسلح، وللظفر بالنصر بأقل خسائر، هذا في النزاعات المسلحة التقليدية، أما فيما يخص موضوع بحثنا، فيبدو الموضوع مختلف نوعاً ما، فلا يشترط وجود طرفين

متحاربين في أثناء إعداد أو تنفيذ الهجمات السيبرانية، فضلاً عن أنها في الغالب تحمل طابعاً وقائياً ضد الخصم المستهدف من الهجوم أن الأثر المترتب في اللجوء إلى الهجمات السيبرانية، يختصره الخبير الروسي "ديميتري كريجوروف" بأنه يتجسد في التهديد على المستوى العسكري والسياسي، فضلاً عن التهديدات الإجرامية والإرهابية التي يمكن لمجموعات من غير الدول تبنيها لأجل الحصول على مزايا سياسية أو اقتصادية، فركزوا عليه بالبحث والتحليل في نطاق النزاعات، وقد تنبه إلى هذا الموضوع الكثير من المختصين، المسلحة عموماً. (الفتلاوي، 2016)

أنواع الهجمات السيبرانية:

أصبح النظام الدولي ظاهرة متعددة في أبعادها ونطاق تأثيرها وملامحها، مما فرض المزيد من التعقيد على ظاهرة الهجمات السيبرانية "الإرهاب الإلكتروني"، التي تنطوي على كثير من الصعوبات والتحديات التي تتعلق بمدى إمكانية إدراج استخدام القوة بصورتها المرنة داخل الفضاء الإلكتروني في الإطار القانوني الذي يتعامل مع استخدام القوة "الصلبة" في العلاقات الدولية، وما ورد في ميثاق الأمم المتحدة في المادة (84) الفقرة (9) في ضوء الهجمات السيبرانية "القانون الدول أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة، أو استخدامها ضد سلامة الأراضي، أو الإستقلال السياسي ألية دولة أو على أي وجه آخر ال يتفق ومقاصد الأمم المتحدة، ووضع ميثاق الأمم المتحدة شروط الإستخدام القوة وردت في المادة (50) فقرة (22) من الميثاق ويمكن القول إن الهجمات السيبرانية تنقسم إلى ثلاثة مستويات هي:

1. حرب المعلومات الشخصية (التجسس الإلكتروني).

التجسس الإلكتروني: (espionage Cyber) هو القيام المخز باختراق شبكة أو جهاز إلكتروني بهدف سرقة المعلومات منه والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء أكانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، وهو ما يترتب عليه آثار إستراتيجية فادحة في الطرف المستهدف.

ويوصف هذا المستوى تجاوزاً للحدود بأنه وصية الخصائص الإلكترونية الفردية؛ مما يشكل اعتداء على الحقوق الشخصية للفرد، وانتهاكا لحرمة الحياة الخاصة، ومنها سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات أو قيام أحد الأشخاص بتكوين ملف عن طريق الحاسب الآلي يحتوي على خصائص معلومات تخص شخص آخر بغير علمه أو إذنه، أو العبث بالسجلات الرقمية وتغيير مدخلاتها المخزونة في قواعد البيانات، ولأن هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، أصبحت العديد من الدول تلجأ إليه، إما في خالل أوقات النزاعات السياسية والتوتر السياسي مع دول أخرى، أو في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية ومن أبرز أمثلة التسجيل الإلكتروني الذي تقوم به دول ضد أخرى، ما ورد في تقرير لجنة التحقيقات التي شكلها البرلمان الأوروبي والذي اتهم الولايات المتحدة باستخدام شبكة تسجل إلكترونية تحت اسم (network Echelon) والتي تأسست أثناء الحرب الباردة؛ للتسجيل وسرقة المعلومات الصناعية الخاصة بالصناعات الأوروبية، وتجدر الإشارة إلى أن الدول ليست هي الهدف الوحيد لمثل هذه الهجمات، أيضاً الهجمات، والشركات سواء أكانت التجارية أم الإعلانة والمنظمات غير الحكومية، التي أصبحت تتعرض هي الأخرى لعديد من عمليات التجسس الإلكتروني.

2. حرب المعلومات بين الشركات والمؤسسات:

يدور هذا المستوى ضمن إطار المنافسة بين الشركات والمؤسسات استبقوا ما ق كل شيء لتعطيل المنافل، وتهديد أسواقه، بحيث تقوم شركة معينة باختراق النظام المعلوماتي لمنافستها وسرقتها، وتفاصيل انتائج أبحاثه وتدمير البيانات الخاصة بها واستبدالها ببيانات أخرى غير صحيحة .

3. حرب المعلومات العالمية (الحرب السيبرانية)

تشير الحرب الإلكترونية أو الحرب السيبرانية إلى تلك الحرب التي تتم إدارتها في مجال الفضاء الإلكتروني، والتي يتم فيها استخدام الآليات والأسلحة الإلكترونية في الهجوم، ويكون هذا الهجوم موجه الإرسال إلى أجهزة الحاسب الآلي، أو الشبكات الإلكترونية الخاصة بالعدو أو الأنظمة الإلكترونية التي تدير الدولة وما تحتوي عليه من ؛ معلومات بهدف عرقلة الخصم عن استخدام هذه الأنظمة والأجهزة والشبكات أو تدميرها بالكامل وهذا المستوى يمثل الحروب التي تحصل بين بعض الدول أو، الذي قد تشنه القوى الاقتصادية العالمية على بلدان بعينها سرقة أسرار الخصوم أو الإغواء وتوجيه، تلك المعلومات توجيهها مضاداً لمصالحهم، حيث إن الدولة التي تمتلك هذه التكنولوجيا تحظى بالتفوق في ميدان المعركة ؛ من خلال استخبارات نوعية وشاملة، وقدرة هجومية دقيقة وخاطفة، وقدرة على الدفاع عن بنيتها التحتية الحيوية، إلى جانب قدرات عالية على السيطرة والتحكم وما يتبع ذلك، إلا إن التطور في مجال تكنولوجيا المعلومات، وعلى وجه الخصوص الحواسيب، ووسائل الاتصال، والشبكات الإلكترونية، جعل من الممكن القيام باستهداف الخصم فرداً أو دولة أو مؤسسة، بأساليب جديدة تلائم طبيعة ذلك

التطور، وبنحو عام يمكن تحديد ثلاثة مستويات رئيسة للحرب السيبرانية أو الهجمات السيبرانية، هي: (حكيم، 2018)

المستوى الأول: ويتمثل في تلك العمليات المصاحبة للحروب التقليدية؛ لتحقيق التفوق المعرفي، كمهاجمة نظام الدفاع الجوي والذي يؤدي إلى خسائر إستراتيجية واسعة النطاق نتيجة الأهمية الدفاع الجوي بالنسبة للدول.

المستوى الثاني: فيتمثل في الحرب الإلكترونية المحدودة، والتي تتعرض فيها البنية التحتية، والأهداف المدنية للهجمات السيبرانية.

والمستوى الثالث: ويتمثل في الحرب الإلكترونية غير المحدودة، والتي يسعى من خلالها القائم بالهجوم إلى تعظيم الآثار التدميرية للبنية التحتية، حيث يؤثر سلبا في البناء الاجتماعي للدولة كمهاجمة أسواق رأس المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف التي يترتب عليها آثار تدميرية واسعة النطاق، ويكون الهدف من هذا النوع من الحروب، هو توسيع نطاق الخسائر المادية قدر الإمكان.

إن الهجمات السيبرانية تستهدف معلومات أو نظم معلومات محددة عند الطرف المراد مهاجمته؛ وذلك لزيادة قيمة تلك المعلومات أو نظمها بالنسبة للمهاجم، أو تقليل قيمتها بالنسبة للمدافع، أو بهما معا، وذلك لأن قيمة المعلومات ونظمها هو المكيال لمقدار استحواذ المهاجم أو المدافع للمعلومات ونظمها على أن الهدف كأهداف مالية يتشك يسعى المهاجم في حربه لتحقيقه قد ضمن يقوم بسرقة وبيع سجلات لحسابات مصرفية، وقد تكون تلك الحرب أو حتى لمجرد الإثارة وإظهار القدرات والأهداف السياسية أو العسكرية كما في حالة قرصنة المعلومات، وسائل

الهجمات السيبرانية الأسلحة الإلكترونية تشير الأسلحة الإلكترونية، أو وسائل الهجمات السيبرانية إلى تلك الأدوات التي يتم استخدامها للتهديد إحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهيكل الإلكترونية، وتختلف هذه الأسلحة والأدوات من حيث درجة خطورتها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى معقدة يمكن من خلالها اختراق النظام واختراق، النظم حدث أضرار بالغة به قد تصل إلى تدميره كلياً أو توقفه، عن العمل الكلي وفي النقاط الآتية، سيتم توضيح أبرز الوسائل التي تعد أسلحة للحرب السيبرانية، والاعداد تكثر إستخداما على الساحة الدولية، وذلك على النحو التالي :

4. استخدام برامج القنابل المنطقية "Bombs Logic" وتعد بمثابة برنامج ينفذ في لحظة محددة أو في فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام ؛ بغية تسهيل تنفيذ العمل غير المشروع، كإدراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محال الاعتداء كأن تسعى قنبلة منطقية إلى البحث عن حرف (A) أي سجل ي تضمن أمراً بالدفع، وعندما تكتشفه، تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل.

5. استخدام برامج الدودة "Software Worm" وهذه البرامج تعرف بأنها تستغل أية فجوات في نظم تشغيل الحاسب الآلي لتنتقل من حاسب إلى آخر، مغطية شبكة بأكملها؛ لتحديث آثار تخريبية للملفات، والبرامج، ونظم التشغيل، وبروتوكولات الإتصال.

6. استخدام فيروسات الحاسب الآلي "Virus Programs" وهذه تعد من أكثر الوسائل انتشار وهي بمثابة مجموعة من التي تنتج لنفسها نسخ التعليمات

المرمزة والمطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات ومكونات للنظام المنفذ لتقوم في مرحلة فه المركز القومي محمية بالتحكم في أداء النظام الذي أصابته، وقد عرف للحاسب الالى في الولايات المتحدة الأمريكية بأنه برنامج مهاجم بأسلوب يماثل إلى حد يصيب أنظمة الحاسبات، كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان هذا البرنامج يقوم حيث بالتجول في الحاسب الالى باحثا عن برنامج غير مصاب وعندما أحدها يجد ينتج نسخة من نفسه لتدخل فيه، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس، ومن أهم خصائصه قدرته الفائقة على الاختفاء، والاختراق والانتشار وقدرته على تدمير نظام الحاسب الالى بأكمله "Denial of Service" الخدمة إنكار هجمات "Dos" وهي عبارة عن هجمات إلكترونية تتم بإغراق المواقع بسيل من البيانات غير الالزامية التي يجري إرسالها ببرامج متخصصة تعمل فتؤدي إلى بطئ نشرها في الخدمات أو ازدحام في المرور التي يصعب على المستخدمين إليها إليها.

7. الهجوم الإلكتروني: كالتشويش والخداع الإلكتروني، والصواريخ المضادة للإشعاع الكهرومغناطيسي، والقيام بالتجسس على الهدف؛ لسرقة معلومات سرية، بغض النظر عن الأهداف والتي قد تكون اقتصادي تجارة عسكرية بين دول بين الشركات، أو إستراتيجية أو معينة، ومن تلك العمليات أيضا التعدي على الملكية الفكرية، وقرصنة المعلومات، كسرقة البرامج الحاسوبية، وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي، خاصة وأن وجود شبكة الإنترنت قد أدى إلى توسيع انتشار مثل تلك العمليات؛ لسهولة النشر والتوزيع على هذه الشبكة وبصفة عامة يمكن تحديد مجموعة من الخصائص التي تتسم بها وسائل السبائية وأسلحتها بأنواعها المختلفة.

ويمكن تحديد هذه الخصائص بما هو آتٍ:

أ. تتسم وسائل السيرية وأسالتها بخضوعها لعمليات تحديث وتطوير مستمرين مما يزيد في قدرتها التدميرية وفاعليتها في شن الهجمات الإلكترونية.

ب. سهولة الإستخدام ومتوفرة على نطاق واسع، بحيث يمكن ها من الإنترنت أو شراؤها، وتمكن مُستخدميها من تحميل القيام بهجمات معقدة تتخطى مستوى قدراتهم الحقيقية .

ت. تتسم بدقتها وفاعليتها وقدرتها على اختراق أكثر أنظمة الحماية تعقيداً، كما أنها قادرة على إصابة أنواع مُختلفة من الأجهزة الإلكترونية، سواء أكانت أجهزة الحاسب أم مقدم الخدمة، أم أي جهاز متصل بشبكة إلكترونية.

الآثار الناشئة عن الهجمات السيرية:

ليس لآثار الهجمات السيرية حدود، فبأمكنها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية أو تعطيل وسائل النقل براً وبحراً وجواً، أو تغيير مسار الرحلات، إضافة لتعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها، وكذلك تعطيل أنظمة التحكم والتشويش على الصواريخ والطائرات وتغير مسارها، أو تعطيل أنظمة الدفاع أو حواسيب أمن المعلومات وتصل قد ارتها لتعطيل أجهزة الاتصالات بكل أنواعها، ناهيك عن اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات. (ايهاب، 2020)

وتالياً أهم الآثار الناشئة عن الهجمات السيرية في عدة مجالات فيما يلي:

الآثار الناشئة عن الهجمات السيبرانية في المجال العسكري :

لقد لعبت التكنولوجيا دوراً مهماً في المجال العسكري، حيث تعتمد عليها معظم الأنظمة العسكرية اليوم وتمثل الميزة النسبية للتكنولوجيا في قدرتها على الوحدات العسكرية معاً، لتسمح بتبادل المعلومات وتدفقها بسهولة، والسرعة في إعطاء الأوامر العسكرية، والقدرة على تدمير الأهداف عن بعد.

وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة السيبرانية المستخدمة آمنة لدرجة كافية فقد تؤدي الهجمات السيبرانية ضد الشبكات الخاصة بالمؤسسات الأمنية والعسكرية إلى السيطرة عليها، مما يؤدي إلى وقوع ضحايا في صفوف المقاتلين والمدنيين، وتهديد السهام والأمن الدوليين، وبالتالي إن الهجمات السيبرانية على المجال العسكري لها نفس النتائج الناجمة عن الاستخدام المادي للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدولة، ووقوع وفيات تين العسكريين والمدنيين.(غيث،2020)

الآثار الناشئة عن الهجمات السيبرانية في المجال الاقتصادي:

أصبحت صناعة تكنولوجيا المعلومات والاتصالات مورداً اقتصادياً مهماً للكثير من الدول، حيث أسهمت ثورة تكنولوجيا المعلومات والاتصالات في جعل أصحاب القرار يتخذون قرارات استثمارية رشيدة وبالتالي ساهمت في زيادة معدلات التنمية الاقتصادية، ومن الأمثلة على استخدام التكنولوجيا في المجال الاقتصادي ما يلي: إعلانات المنتجات الجديدة، والأخبار الصحفية عنها، ومعلومات ترويجية حول مبيعات محددة وخاصة عرض ودراسه السوق، وأبحاث العملاء، وجمع المعلومات الخاصة بخدمة العملاء، والتسويق الإلكتروني. فأى هجوم سيبراني على

هذا المجال سوف يؤثر ويجلب العديد من الآثار السلبية وسيكون المدنيون عاطلين عن العمل وغير محميين، وستتعطل العمليات من منطقة إلى أخرى مسببة تدهوراً اقتصادياً على مستوى الدولة، ومثال ذلك الاحتيال في تحويل الأموال بالوسائل السيرية، وسرقة الأرصفة وتحويلها إلى أنشطة إجرامية. (العتيبي، 2017)

الآثار الناشئة عن الهجمات السيرية في المجال الصحي:

أصبح استخدام أجهزة وبرامج الكمبيوتر في الوقت الحالي دواراً مهماً في تحسين جودة وكفاءة الرعاية الصحية وتقليل تكلفتها، ومن أهم ما تم تطويره فكرة السجلات الطبية الإلكترونية التي تشمل المعلومات الخاصة بالمرضى والتاريخ الطبي والعلاجات السابقة، والأدوية المستخدمة سابقاً، وحالات الحساسية، والأعراض ونتائج الأمراض المختلفة والاختبارات التشخيصية، وكذلك مواعيد زيارة الأطباء أو المستشفيات والعلاجات التي تلقاها المرضى، وصور الأشعة التشخيصية والموافقات القانونية. (العتيبي، 2017)

ولقد أثرت التكنولوجيا الجديدة بشكل كبير على المجال الصحي، فظهر مفهوم الطب عن بعد الذي يهدف بشكل أساسي إلى تقديم الخدمات الطبية وخفض التكاليف بشكل أساسي في الدول الفقيرة أو المناطق الريفية بما يتماشى تلك المقدمة في المدن الكبرى والعواصم، وتقليل نفقات انتقال المريض والتواصل بين المريض والطبيب .

الآثار الناشئة عن الهجمات السيرية في المجال البيئي:

لقد تم استخدام أنظمة الاستشعار عن بعد ونظم المعلومات الجغرافية في مجال الحفاظ على البيئة، حيث تساهم في دراسة تلوث المياه والهواء وسطح الأرض من خلال

صور الأقمار الصناعية بعد معالجتها بجهاز الكمبيوتر، في تحديد مصادر التلوث ومراقبة الامتداد الموضعي للتلوث، خاصة أثناء حدوث تلوث جارئ معين، بالإضافة إلى دراسته تركيز هذا التلوث، وسرعة جريانه وتدفقه، ومقدار تشتته أيضاً.

وتستطيع أجهزة قياس الإشعاع متناهي القصر الدقيقة في الكشف عن تسرب النفط والبقع الزيتية. وفيما يتعلق بالكوارث الطبيعية، يمكن لصور الاستشعار عن بعد أن توفر معلومات دقيقة وسريعة عن مثل هذه الكوارث قبل أو أثناء حدوثها أو بعد حدوثها توقت قصير، كالفيضانات والأعاصير، وحرائق الغابات والكوارث والانفجاعات البركانية، ويظهر جلياً أهمية التكنولوجيا في مجال حماية البيئة من التلوث والحد منه بأسرع وقت، وأي هجوم سيرانى على هذا المجال سوف يتسبب في الكثير من الدمار والاذى للنظام البيئى (العتبى، 2017).

ونستنتج أن آثار الهجمات السيرانية على كل من المجالات العسكرية والاقتصادية والصحية والبيئية، خطيرة جداً وقد تؤدي إلى كوارث كبيرة خاصة إن كانت نتائجها مماثلة للاستخدام المادى للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدول، ووقوع وفيات بين العسكريين والمدنيين، وإحداث اضطراب كبير في المجال الصحى والاذى والدمار للنظام البيئى، لذا نؤكد مرة أخرى على ضرورة الحد من استخدام الهجمات السيرانية.

التكلفة البشرية المحتملة للعمليات السيرانية:

استخدمت العمليات السيرانية خلال النزاعات المسلحة لدعم العمليات الحركية أو بجانبها، وقد يوفر استخدام العمليات السيرانية بدائل لا تتيحها سائر وسائل وأساليب القتال، فمن ناحية، قد تمكن العمليات السيرانية غير أنه ينطوي

على مخاطر أطراف النزاعات المسلحة من تحقيق أهدافها دون إلحاق أضرار بالمدنيين أو التسبب في أضرار مادية بالبنية التحتية المدنية.

ومن ناحية أخرى، تبين العمليات السيرية الأخيرة التي نفذت أساساً خارج سياق النزاعات المسلحة أن الجهات الفاعلة المتطورة أصبحت غير قادرة على تقديم الخدمات الأساسية للسكان المدنيين، ويمكن للأطراف المتحاربة التسلل إلى نظام ما عن طريق العمليات السيرية وجمع البيانات أو تهريبها أو تعديلها أو تشفيرها أو اتلافها، ويمكن أيضاً استخدام نظاماً حاسوب مخترق لتشغيل العمليات التي يسيطر عليها هذا النظام أو تغييرها أو معالجتها بطريقة أخرى. ويمكن تعطيل مجموعة متنوعة من "الأهداف" في العالم الحقيقي أو تغييرها أو اتلافها، مثل الصناعات والبنية التحتية والاتصالات السلكية واللاسلكية وأنظمة النقل، أو الأنظمة الحكومية أو المالية، وينتاب اللجنة الدولية القلق خاصة إزاء التكلفة البشرية المحتملة للعمليات السيرية ضد البنية التحتية المدنية الأساسية، بما في ذلك البنية التحتية للخدمات الصحي.

وكشفت الهجمات السيرية على مدار السنوات الأخيرة مدى ضعف الخدمات الأساسية، وأن هذه الهجمات أصبحت أكثر تواتراً وأن حدتها تزداد بسرعة أكبر مما توقع الخبراء، وعلاوة على ذلك، لا يزال هناك مجالات لا يعرف عنها سوى القليل جداً: القدرات والأدوات السيرية الأكثر تعقيد والتي طورت بالفعل أو الجاري تطويرها؛ وكيف يمكن أن تتطور التكنولوجيات؛ ومدى اختلاف استخدام العمليات السيرية خلال النزاعات المسلحة عن التوجهات التي صدت حتى هذا الوقت، إضافة إلى ذلك، تثير خصائص الفضاء السيري مخاوف بعينها، وتنطوي

العمليات السيرية على خطر التصعيد وإلحاق الأضرار البشرية، إذ يصعب على الطرف المستهدف معرفة ما إذا كان المهاجم يهدف إلى جمع المعلومات الاستخبارية أو إلحاق ضرر أكبر، مما يؤدي إلى رد فعل من الطرف المستهدف بقوة أكبر من اللازم تحسباً لوقوع السيناريو الأسوأ وتنتشر الأدوات السيرية بطريقة فريد، ويمكن بمجرد استخدامها الاستفادة منها لأغراض أخرى وتوظيفها على نطاق واسع من قبل الجهات الفاعلة بخلاف المطور والمستخدم الأصلي. (الصليب الأحمر الدولي، 2019)

العقيدة الأمنية الجديدة:

إن حالة انعدام الثقة واليقين في العلاقات الدولية، هو ما يشجع تزايد النزاعات في العالم، إضافة إلى التطورات السريعة في الفضاء السيرياني، جعلت الدول تسارع إلى تبني تغييرات في العقيدة الأمنية، وذلك بإدراج القوة السيرية كمحدد رئيس ملدى قوة الدولة، وقدرتها على حسم النزاعات لصالحها وكمثال على ذلك، نجد أن العقيدة الروسية الجديدة، تكشف أنه تمت إضافة بند جديد يخص تهديدات الأمن السيرياني في المجالين العسكري والإقتصادي، ووفقاً للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي بوتين، فإن إحدى التهديدات الرئيسية لروسيا تتمثل "بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا"، أحد الأهداف الرئيسية لوضع هذه العقيدة للأمن السيرياني، هو "الردع الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات. (زروق، 2019)

لقد ارتبط تصاعد الصراع بين روسيا والدول الغربية بقيادة الولايات المتحدة، خلال السنوات الماضية باستدعاء متنام لحرب المعلومات كأحد للمداخل الهامة للتأثير في مسارات الصراع، كما يعتقد سميث "Smith" في دراسة له بعنوان "كيف تستخدم روسيا الحرب السيبرانية؟"، أن روسيا "تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل: الاستخبارات، والتجسس المضاد، والخداع، والتضليل، والحرب الإلكترونية وتدمير الاتصالات وأنظمة دعم الملاحه، والضغوط النفسية، فضلاً عن الدعاية وإلحاق الضرر بنظم المعلومات" ويفترض أنتونوفيتش "Antonovich" أن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار، مهما كانت طبيعتها، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي، وفي الجهة المقابلة، نجد أن منظمة "حلف شمال الأطلسي NATO" سعت بدورها إلى تحديث عقيدته الأمنية، استجابة للتغيرات الحاصلة في طبيعة التهديدات وطبيعة الحرب، حيث أقر مجموعة من النقاط الأساسية من بينها: (jana,2013)

أ. أن الدفاع السيبراني يمثل جزءاً أساسياً من الدفاع الجماعي للحلف.

ب. الفضاء السيبراني يمثل مجالاً لعمليات الحلف.

ت. بناء قدرات سيبرانية تعد مهمة أساسية للحلف وحلفائه .

بالإضافة الى ذلك، نجد كال من الصين، إسرائيل، بريطانيا، فرنسا، والولايات المتحدة الأمريكية إيران، وكوريا الشمالية، قد طورت كل منها عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحاً للعمليات العسكرية، كما أوجدت قيادة خاصة ومستقلة لقيادة العمليات السيبرانية.

الفصل الرابع

الحروب السيبرانية

تمهيد:

تعد أنظمة الكمبيوتر الحيوية إحدى تعريفات الحروب السيبرانية، وهناك جدل كبير بين الخبراء فيما يتعلق بتعريف الحرب الإلكترونية، وحتى إذا كان هذا الشيء موجوداً. هناك رأي مفاده أن مصطلح "الحرب الإلكترونية" تسمية خاطئة، حيث لا يمكن وصف أي أعمال إلكترونية هجومية حتى الآن على أنها "حرب". وإن "الحرب الإلكترونية" هي تسمية مناسبة للهجمات السيبرانية التي تسبب ضرراً مادياً للأشخاص والأشياء في العالم الحقيقي.

ولئن كان هناك نقاش حول كيفية تعريف واستخدام "الحرب الإلكترونية" كمصطلح، العديد من البلدان بما في ذلك الولايات المتحدة، المملكة المتحدة، روسيا، الهند، باكستان، الصين، الكيان الصهيوني، إيران، وكوريا الشمالية قدرات إلكترونية نشطة للعمليات الهجومية والدفاعية. بينما تستكشف الدول استخدام العمليات السيبرانية وتجمع بين القدرات، وتزداد احتمالية المواجهة الجسدية والعنف كنتيجة لعملية إلكترونية، أو جزء منها، ومع ذلك، فإن تلبية حجم الحرب وطول أمدها أمر غير مرجح، وبالتالي يبقى الغموض قائماً.

ولنلاحظ بأن أول عمل عسكري حربي تم استخدامه رداً على هجوم إلكتروني أسفر عن خسائر في الأرواح في 5 أيار 2019، عندما استهدف جيش دفاع الكيان الصهيوني مبنى مرتبطاً بهجوم إلكتروني مستمر ودمره وهناك جدل مستمر حول كيفية تعريف الحرب السيبرانية، ولا يوجد تعريف مطلق متفق عليه على نطاق واسع بينما

يستخدم غالبية العلماء والجيش والحكومات تعريفات تشير إلى الجهات الفاعلة التي ترعاها الدولة والدول، و قد تشمل التعريفات الأخرى الجهات الفاعلة غير الحكومية، مثل الجماعات الإرهابية، الشركات والجماعات السياسية أو الأيديولوجية المتطرفة ونشطاء القرصنة والمنظمات الإجرامية عبر الوطنية اعتمادًا على سياق العمل.

المبحث الأول: ماهية الحرب السيبرانية

تكمن خطورة الحروب السيبرانية في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء السيبراني، لا سيما في البنى التحتية المعلوماتية، ولا شك أن ازدياد الهجمات السيبرانية يعني إمكانية تطورها لتصبح سالحا حاسما في النزاعات بين الدول في المستقبل:

ويعد مفهوم الحرب السيبرانية لا يوجد إجماع على تعريف محدد ودقيق المفهوم الحرب السيبرانية فيعرفها كل من "ريتشارد كالك" و"روبرت كناي" على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".

ويعرفها شاكران "Shakarian" امتداد للسياسة من خلال الاجراءات المتخذة في الفضاء السيبراني من قبل دول أفاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي، ويقترح آخرون أن يتم التركيز بدلاً من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء السيبراني، ويحددون مستوياتها كالتالي: القرصنة السيبرانية: وتقع في المستوى الأول، ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية، أو بتعطيل الحواسيب الخادمة "Servers" من خلال إغراقها بالبيانات.

الجريمة السيبرانية والتجسس السيبراني فيقعان في المستوى الثاني والثالث، وغالبا ما يستهدفان الشركات والمؤسسات، وفي حالات نادرة بعض المؤسسات الحكومية.

الإرهاب السيبراني: ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون .

الحرب السيبرانية: وهي المستوى الأخطر للنزاع في الفضاء السيبراني، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجّهات المدنيين في مسرح العمليات الإلكتروني.

خصائص الحروب السيبرانية:

من المتوقع أن تصبح الحرب السيبرانية نموذجاً تسعى إليه العديد من الجهات نظراً للخصائص العديدة التي تنطوي عليها، ومنها مايلي: (زروق، 2019)

أ. حروب اللاتناظرية " **Asymmetric** ": فالتكلفة المتدنية نسبياً للملاذات الدالة، يعني أن ليس هناك حاجة لدولة معينة أو منظمة ما لقدرات ضخمة لتشكل تهديداً خطيراً نوحقيقاً على دولة مثل الولايات المتحدة الأمريكية.

ب. تمتع المهاجم بأفضلية واضحة: فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وفي بيئة مماثلة يتمتع المهاجم بأفضلية، ومن الصعوبة نجاح عمليات الدفاع.

وهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحس كاستهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي للمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى دمار هائل، وقد ميز التاريخ العالمي للحروب بوجود حرب تميز كل حقبة زمنية وتعتبر الأعظم في تلك الحقبة، فكانت على مر العصور والسنوات حروب ميزت كل عصر، بدءاً من الحروب التقليدية وصولاً للحروب الكيماوية والنووية.

وتتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة

الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة الكترونية جديدة تالئم طبيعة السباق الإلكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء الأجهزة الاستخباراتية، وعليه فأن احد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالأستناد إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول أن الحرب التقليدية وفقاً للسيبرانية، هي الحرب التي تستخدم فيها الأسلحة غير لآثار المترتبة على استخدام هكذا نوع من الأسلحة والمتمثلة بالتدمير واسع النطاق. (سعود، 2018)

وتعرف الأسلحة غير التقليدية وفقاً للجنة الأسلحة التقليدية للأمم المتحدة والصادر عام 1991 بأنها: اسلحة الانفجارات الذرية والأسلحة المصنوعة من مادة ذات نشاط اشعاعي واسلحة الفتك الكيميائية والبيولوجية واي نوع من الأسلحة الاخرى التي يتم تصنيعها في المستقبل والتي تتشابه خصائصها في الاثر التدميري مع القنبلة الذرية أو الأسلحة الاخرى ويرتبط مفهوم الحرب السيبرانية بانه عبارة عن هجمات الكترونية بقيادة عسكرية تقوم باختراق الأنظمة الإلكترونية العالمية وكل ما يعتمد على التكنولوجيا، لتضر بالحواسيب والأجهزة التي تستخدم شبكة الإنترنت العالمية والتي قد تفضي لنتائج كارثية، مثل سرقة بيانات خاصة، وغيرها من الكوارث التي قد تكون عالمية مثل الحروب النووية وغيرها. (سعود، 2018)

تاريخ الحرب السيبرانية

يمكننا القول بأن أول استخدام لمصطلح "السيبرانية" قد كان في الربع الأول من النصف الثاني من القرن الماضي، والذي ذكره الكاتبان كلاينس وكلاينس في مقالاتهم للإشارة بين الإنسان والالكترونيات معاً. وبعد ذلك كان مدى استخدام هذا المصطلح ضئيل الى حدٍ ما.

وفي عام 1983 أصدرت هوليود فيل العايب الحروب "War Games" والذي يروى قصة فتى هاوي وعبقري في الحاسوب، بحيث يستطيع ان يخترق الجهاز الرئيسي للجيش الأمريكي، مسبباً بذلك ازمة عالمية كادت ان تنتهي بحرب عالمية ثالثة، وكان هذا الفيلم بمثابة شرارة التي دفعت بالكثيرين ليتساءلوا تجاه إمكانية تحقيق ما جاء بالفلم فعلياً، وهل هو مستحيل ام لا! ولم يدركوا ان الأمر قد يكون بمثابة عرض بسيط لما سيحدث لاحقاً بفعل الحرب السيبرانية التي ستغزو العالم أجمع.

تطور الحرب السيبرانية:

بعد الانتشار الواسع والكبير والسريع للكمبيوتر والإنترنت من أمريكا والدول المتقدمة لباقي دول العالم، بدأت المخاوف تتزايد لدى الجميع بإمكانية تحقيق الأمر.

ثم أصدرت لجنة أمريكية مختصة بحماية البنية الأساسية تقرير عام 1997م دعت فيه للتفكير بشكل مغاير عن الصورة النمطية التي يفكر بها الجميع بالأمن عموماً والسيبراني خصوصاً وتداعياته على الوضع العالمي وأثاره في ظل التطور الهائل للتكنولوجيا الرقمية.

وفي ظل كل هذا التطور الخبر والمخاوف التي تحف العالم من الحرب السيبرانية وخطارها، قامت الولايات المتحدة بتشكيل " الفريق الأحمر" المختص بكشف الثغرات التي تتعرض لها الشبكة الرقمية الأمريكية واعتبر بمثابة الجيش السيبراني لأمریکا، حيث اكتشف كافة الثغرات التي شكلت نقطة ضعف للولايات المتحدة.

وفي نفس العام تعرضت الولايات الأمريكية لهجومين كبيرين الأول وهو الشروق الشمسي والذي اكتشف لاحقاً أن فاعله هما صبيان أمريكيان لم تتجاوز أعمارهم السادسة عشر، حيث كانا يتسابقان فيمن يستطيع أن يخترق البنتاجون أسرع من الآخر، أما الهجوم الثاني والذي أطلق عليه اسم متاهة ضوء القمر وهو ما يمكننا اعتباره هجومي وعدائي أكثر من الأول حيث استمر القراصنة فيه لعدة أشهر في اختراقاتهم وكانت روسيا هي وراء هذه الهجمة الشرسة، التي راح ضحيتها الكثير من المعلومات والملفات التي تقدر بالملايين، ومن هذه النقطة يمكننا اعتبار أنها بداية الحرب السيبرانية الفعلية.

ذروة الحرب السيبرانية:

لقد زادت هجمات الحرب السيبرانية حتى أوائل القرن الحالي حيث بدأ مصطلح الحرب السيبرانية بالظهور بشكل أكبر ومتوسع عام 2003 عندما قامت مجموعة من القراصنة الالكترونيون السوريين التابعين للنظام السوري بشن هجمات الكترونية على مواقع عالمية، ونشر اخبار كاذبة عليها تخص البيت الأبيض، وبعد ذلك توالى الهجمات المختلفة والتي كانت تحت غطاء الحرب السيبرانية.

وكانت الدول العظمى والأكثر تطوراً هي الأشد عرضة لهذه الهجمات والمتمثلة بالولايات المتحدة الأمريكية وروسيا وغيرها من الدول العظمى، وقد تعرضت

الولايات المتحدة التي تعرضت في عام 2014 لحوالي 100 ألف هجمة إلكترونية واختراقات متعددة، ويذكر أن القراصنة لم يكن يكتشف أمرهم في بداية الهجمات لفترات طويلة بعد حدوث الهجمة، حيث كان الأمر في بدايته صعب نوعاً ما.

أهداف الحرب السيبرانية

امتازت الحرب السيبرانية بأنها ذات أهداف بعيدة المدى، فلا يقف مدى خطورتها على حدٍ معين، وليس لأضرارها نطاق محدد، وتمثلت أهدافها في أنها:

(<https://cyberone.com>)

1. تعتبر هجمات عابرة للحدود، فلا زمان ولا مكان يوقفها.
2. يمكنها أن تصل لأي مكان في العالم بسرعة خيالية.
3. دمارها شديد الفتك، فقد تفجر محطات طاقة نووية، وقد تعطل كهرباء مدن كاملة.
4. إضافة لأنها قد تصل لأبعد من ذلك، والتي قد تعطل أنظمة تحكم كبيرة، وتغير مسارات الصواريخ وتشوش عليها، وقد يتم اختراق بنوك وسرقتها ويتم التلاعب بتحويلات البنوك من خلالها.
5. تؤدي هجمات السايبر لتعطيل رحلات جوية وبحرية وبرية وتغير مسارها.

آثار الحرب السيبرانية ومدى خطورتها على العالم:

لم تتوقف آثار الحرب السيبرانية على كونها حرب إلكترونية، بل تعدى مدى خطورتها الحدود الإلكترونية ووصلت لأبعد ما يتصوره العقل من حدود. فلم تكتفي

بالعالم الافتراضي، حيث تعدته للواقع ووصلت لاماكن ونقاط لا يمكن التهاون فيها، ولعل من أبرز آثار الحرب السيبرانية:

- أ. تدمير أنظمة دولية وإلحاق اضرار بالغة الخطورة بها.
- ب. في الحرب السيبرانية بالعادة فإن الضحايا بالدرجة الأولى هم المدنيين، سواء باستهدافهم بشكل مباشر او من خلال العالم الافتراضي.
- ت. من آثار الحرب السيبرانية أن ضررها سيكون أكبر من نفعها، والأمر الذي سيجعل العالم بأسره في وجه المدفع.
- ث. تأثير الحرب السيبرانية لن يقتصر على واقع الكتروني او سياسي او عسكري، بل وبلا شك سيطال أنظمة الرعاية الصحية، التي أصبحت تعتمد على العالم الرقمي في اغلب اعمالها.
- ج. قد تتصاعد الأمور في الحرب السيبرانية، ويصل مدى خطورتها لحد الحرب النووية، وهو ما يجعل خطر هذه الحرب كارثي لا محالة.

أشكال الحرب السيبرانية:

كانت الحروب على مر السنين الطويلة بمثابة الكوارث التي هددت أمن الملايين حول العالم، ولكن مع التطور الكبير لم يعد الأمر يقتصر على الحروب التقليدية التي عايشناها واستخدمت السلاح الفعلي، ولكن تطورت لان تصل للحرب السيبرانية التي تستطيع ان تدمر الكثير دون ان يتم إطلاق رصاصة واحدة ويمكننا ان نعدد أشكال الحرب السيبرانية في مجموعة نقاط وهي: (

(<https://cyberone.com>)

أولاً: الهجمات الإلكترونية، او: "Cyber EA"

وهو استخدام القوة الإلكترونية من قبل مجموعة من القراصنة من أجل ضرب الخصم او العدو وتدميره إلكترونياً والاستيلاء واختراق انظمته الإلكترونية والتلاعب والتحكم بها.

ثانياً: الحماية الإلكترونية، او: "Cyber EP"

وهي عبارة عن كل المحاولات التي تقوم بها الجيوش السيبرانية من أجل حماية الإلكترونيات الخاصة بالدولة وغالباً ما تكون ذات طابع دفاعي يهدف للحماية من الهجمات التي قد تتعرض لها الأنظمة الإلكترونية من أي هجوم مباغت.

ثالثاً: دعم الحرب السيبرانية: "Cyber ES"

وهي مجموعة الإجراءات التي يتم اتخاذها بغرض تقديم الدعم لحماية الأنظمة الإلكترونية في الدولة تحسباً لتعرضها لأي هجوم او تهديد مفاجئ قد يضر بها على المستوى المستقبلي.

الجيش السيبراني:

بدأ أول ظهور لفكرة الجيش الإلكتروني او السيبراني، والذي له الدور البالغ ويمكن اعتباره الأساسي بالحرب السيبرانية عام 2003، في حين ظهرت اخبار على مواقع عالمية لمدة ثواني معدودة، تفيد بوقوع عدة انفجارات في البيت الأبيض واصابة الرئيس آنذاك باراك أوباما إصابة بليغة.

وتعرف الجيوش الإلكترونية او السيبرانية بكونها عبارة عن مجموعة من الالكترونيون الخبراء في محال البرمجة وتكنولوجيا المعلومات، ويذكر ان هذه المجموعة تكون تابعة لحكومات الدول، وبذلك تكون هذه الجيوش تم انشاؤها

لدوافع سياسية، بحيث يكون عملهم فعلياً خفي ولا يعرفه العامة؛ نظراً لسرية عملهم وحساسيته، وان مهمتهم تركز على الدفاع عن امن الدولة الإلكتروني وشن هجمات الكترونية على الأعداء في حالة الضرورة.

أقوى الجيوش السيبرانية: (<https://cyberone.co>)

لم يقتصر السباق بين دول العالم المتقدمة على سباق التسلح او امتلاك قوة نووية، او حتى امتلاك اعلى الجيوش العسكرية وغيرها من الأمور الواقعية، بل تطور الأمر لأن يكون التسابق الفعلي ضمن مجال الأمن السيبراني، فأصبحت دول العالم تتسابق من أجل بناء اقوى الجيوش الإلكترونية، ومن اقوى الجيوش السيبرانية:

الجيش الأمريكي

حيث أعلن الرئيس الأمريكي السابق دونالد ترامب عن رفع بلاده لمستوى الأمن السيبراني لمستوى قيادة قتالية موحدة، وبذلك تصبح وحدة العمليات الإلكترونية الأمريكية وحدة مستقلة بذاتها وغير مرتبطة او تابعة لأي قوة أخرى.

الجيش الصيني

حيث أنشئت الصين عام 2015 الجيش الأزرق الصيني والمختص بحماية الفضاء الصيني الإلكتروني للجيش من أي هجمات سيبرانية خارجية، ويذكر أن الصين قد تعرضت للعديد من الاتهامات من عدوتها الأولى أمريكا بأنها قامت بعدة اختراقات امنية أمريكية مثل اختراقات لشركة الطاقة النووية الأمريكية، وقد عرف عن الصين بأنها تمتلك أقوى الجيوش الإلكترونية بالعالم.

الجيش الروسي

في عام 2017 أعلنت روسيا عن امتلاكها جيش إلكتروني هدفه حماية الفضاء الإلكتروني الروسي، بحيث يحدد الهجمات التي تتعرض لها روسيا، ويجرب الأبحاث لتحسين قدرته على الحماية الإلكترونية لروسيا.

جيش الكيان الصهيوني

يعتبر الجيش التابع للكيان الصهيوني من أكثر الجيوش ذات قوة إلكترونية كبيرة، ولم يكتفي بكونه يحمي الجيش من الهجمات السيبرانية، بل يعتبر ذو وحدات متعددة متخصصة في مجال الحرب الإلكترونية والتي منها: وحدة الإشارة الموجودة في صحراء النقب، والتي قامت بالعديد من الهجمات الإلكترونية على المنشآت الإيرانية والسورية وغيرها.

الجيش البريطاني

انضمت بريطانيا للحرب السيبرانية عام 2015م، ويذكر أنها تعرضت لهجمات إلكترونية كبيرة وكثيرة، ما دفعها ان تعلن برنامج للتصدي لهذه الهجمات والذي نتج عنه الجيش الإلكتروني البريطاني الذي تتركز مهماته في الدفاع والدرع والتطوير.

المبحث الثاني: تداعيات الحروب السيبرانية على الأمن القومي:

لقد سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، ويمكن طرح أبرزها على النحو الآتي : (مختار، 2015)

1. تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية، سواء كانت مدنية أو عسكرية في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية، تجعل من قوة الدولة المهاجمة سلاح يحسم كل شيء مما يودي إلى السيطرة.

2. تعزيز القوة وانتشارها، عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وأدى إلى عملية انتشار القوة بين فاعلين متعددين

3. عسكرة الفضاء السيبراني، حيث برز في هذا الإطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الإستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة .

4. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب وإجراء المناورات لتعزيز الدفاعات الإلكترونية.

5. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حرباً للمستقبل، حيث تري الدول الكبرى أن من يحدد

مسير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة.

الفضاء الإلكتروني وتغير مفاهيم القوة:

بفضل ثورة المعلومات ومع ظهور الإنترنت ومواقع الويب، ظهرت لدينا بيئة أخرى وهى الفضاء الإلكتروني وعلى الرغم من أن هذه البيئة تختلف عن البيئات الثلاثة "الإقليم البرى، البحرى الجوى" فى كونها من صنع الإنسان، ولكنها تشترك مع البيئات السابقة فى بعض الخصائص وأصبح الفضاء الإلكتروني أحد العناصر المؤثرة فى النظام الدولى بما يحمل من أدوات تكنولوجيا تلعب دور مهم فى عملية التعبئة والحشد فى العالم فضلاً عن التأثير فى القيم السياسية التأثير على نمط القوة، الحرب، الأمن.

أولاً : التغير فى نمط القوة:

عادة ماتترجم الدولة قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها لوسائل مختلفة أهمها "الدبلوماسية، القوة العسكرية، الدعاية، الأدوات الاقتصادية"، ولكن أصبح من المستقر عليه فى مجال العلاقات الدولية، أن مصادر وأشكال القوة تتغير فبالى جانب القوة الصلبة التى تشمل القدرات العسكرية والاقتصادية، هناك تزايد الاهتمام بالأبعاد الغير مادية للقوة، ومن ثم برز دور القوة الناعمة التى تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر لدينا شكل جديد من أشكال القوة وهى القوة السيبرانية وأصبح لديها تأثير على المستوى المحلى والدولى، من ناحية أدت إلى توزيع القوة بين عدد أكبر من الفاعلين مما جعل قدرة

الدولة على السيطرة على هذا الميدان محل شك مقارنة بالمجالات الأخرى للقوة، ومن ناحية أخرى جعلت الفاعلين الأصغر في السياسة الدولية، لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والناعمة في الفضاء الإلكتروني، وهو ما يعنى تغير في علاقات القوة في السياسة الدولية . (علي،2016)

ثانيا : إعادة هيكلة الأمن القومي:

تطور مفهوم الأمن القومي تجاه التهديدات الجديدة الغير تقليدية واتساع مجال الأمن ليمتد من الجانب العسكرى لمجالات أخرى عديدة، وحيث أن أجهزة الحكومة الإلكترونية في العالم في فضاء مفتوح، وعدم وجود حدود جغرافية ” انتفاء السيادة، وتصبح أجهزتها عرضة للعديد من الاخطار تحت دوافع مختلفة، ومن الممكن أن يتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها أو من خارجها عن طريق الهاكرز أو أجهزة الاستخبارات في بلدان معادية عبر تنفيذ الهجمات الإلكترونية بهدف اختراق النظام الأمنى المعلوماتى للحكومة، ولذلك تغير الأمن القومي إلى الأمن السيبرانى التى تسعى الدول إلى حمايته .

ثالثا : التغير في مفهوم الحرب:

لقد تغيرت الحروب التقليدية، وأصبحت الجيوش العسكرية في كافة أنحاء العالم تهتم بحرب المعلومات ودورها في حروب المستقبل، والتى يتوقع الكثير حدوثها في الفضاء الإلكتروني¹ وظهرت مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع وكيف يمكن مواجهته والاستعداد له، مثل الحرب التى تم شنها ما بين جورجيا وروسيا عام 2008، وما بين روسيا واستونيا عام 2007، ولقد قامت العديد من الدول مثل الولايات المتحدة الأمريكية وغيرها من الدول الأخرى

مثل الصين على الرغم من التقدم التكنولوجي لها، ببناء وحدات إلكترونية على شبكات الإنترنت، وإسرائيل بإنشاء 2800 وحدة للحماية من مئات والآلاف القراصنة المحترفين .

القوة السيبرانية والتطبيقات العسكرية في الفضاء الإلكتروني:

تعتمد الدول على قدرتها التكنولوجية وتقدمها في صناعة البرمجيات على خلق ديدان الحاسوب فيروسات برامج خبيثة، تشن بها هجمات على دول تعتبرها معادية، كما نجحت إسرائيل مثلاً بفضل هذا التقدم اقتحام أسواق عالمية وفي مقدمتها السوق الأمريكية، إلى درجة تصل إلى تحذير الخبراء الأمريكيين من الغزو الإسرائيلي لسوق الاتصالات والتكنولوجيا في أمريكا .

وتتمثل عناصر للقوة السيبرانية في الآتي: (علي،2016)

أ. البنية التكنولوجية: تحتاج الدولة في القرن الواحد والعشرين إلى أجهزة كمبيوتر وشبكات اتصالات مرتبطة بأجهزة الكمبيوتر بعضها ببعض وبرمجيات فضلاً عن العنصر البشري المدرب من أجل البنية التحتية " للقوة السيبرانية"، وتستطيع الدولة أيضاً التأثير على الإقليم البري والبحري والجوي من خلال القوة العسكرية المادية بينما الدولة من خلال قوتها المعلوماتية والتكنولوجية تستطيع التأثير في الفضاء الإلكتروني.

ب. الأسلحة السيبرانية: هي برامج تم تصميمها لأداء مهام مختلفة وتشمل :

1. الفيروسات والبرامج الخبيثة: هي برامج تصمم من أجل تنفيذ بعض العمليات مثل الإزالة، التعديل، التخريب، بغرض تدمير أجهزة الدول الأخرى، ولها طريقة معينة في الكتابة، وتستخدم لتعطيل شبكات البنية التحتية، والخدمات لدولة ما،

وإسرائيل استخدمت فيروس "ستاكنت" الذي دمر مفاعل بوشهر في إيران، فيلم "شمعون" الذي دمر شركة أرامكو السعودية.

2. الديدان: هي عبارة عن برامج صغيرة لا تعتمد على غيرها وتتكون عن طريق الشبكات، بهدف قطع الاتصال عن الشبكة، أو سرقة البيانات أثناء تصفح المستخدمين للإنترنت .

3. أحصنة طروادة: هو عبارة عن شفرة مختبئة في برنامج ذو شعبية عالية، ويعمل على نشر دودة أو فيروس، وهو لا يمكن اكتشاف وجوده، ويرسل كلمات المرور الخاصة بالمستخدمين .

4. القنابل المنطقية: هي جزء من أحصنة طروادة، وهي تعمل في ظل ظروف معينة، وتؤدي لمسح جميع بيانات الطرف المستهدف .

وتنقسم العمليات الإلكترونية إلى ثلاث مراحل وهي: (علي، 2016)

1. مهاجمة شبكات الحاسب الآلي: عن طريق اختراق الشبكات بوضع معلومات محرفة لأرباك مستخدمى الشبكات أو الهجمات الإلكترونية، أو نشر الفيروسات، بهدف تعطيل الشبكة، ومن ثم يكون الطرف المستهدف قد دمر تماما "التدمير الفعلى".

2. الدفاع عن شبكات الحاسب الآلي: وهي تتضمن عملية الحماية لشبكات أجهزة الكمبيوتر من أى اختراق خارجى عبر تأمين الأجهزة ببرمجيات معينة (software)، وأيضاً من المكون المادى للشبكات (hard ware).

3. إستطلاع شبكات الحاسب الآلي : وهي القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون تدمير البيانات بهدف الحصول عليها، وهي قد تشمل خطط دفاع عسكرى، أسرار حرب عسكـرية، معلومات

استخباراتية، ويمتد أثرها إلى مدى بعيد مثل رسم خرائط لشبكات الحاسب الآلى واستخدامها مستقبلا في الهجوم الإلكتروني .

أولاً : الردع في الفضاء الإلكتروني:

الردع النووي هو النموذج التقليدي لفهم ودراسة الردع، والقاعدة الرئيسية تقول أنه كلما زادت القوة التدميرية للسلاح، كلما قل استخدامه، وأن الدول الكبرى التي تمتلك أسلحة نووية لا تميل إلى استخدامه أو التلويح باستخدامه لتسوية الصراعات بين الدول، نظرا للقدرة التدميرية العالية وإتباع الخصم نفس الأسلوب من القتال ولذلك تجنب الدول استخدامه، وهذا على عكس الردع في الفضاء الإلكتروني وذلك لأن البيئة التي يعمل فيها الإنترنت مختلفة تماما من عدة جوانب وهما :صعوبة معرفة الطرف المعتدى: يتم من خلال (التتبع، التواصل، المصادقية)

صعوبة وضع الخصم في وضع تهديد: الدول التي تتعرض لهجمات إلكترونية، هي التي تستطيع معرفة مدى نجاح وخسائر هذه الهجمات ولذلك عندما تقوم دولة ما بشن هجوم انتقامي، على دولة أخرى بهدف تحقيق الردع بالانتقام .

صعوبة منع الهجمات الصفريّة : حيث أن الفضاء الإلكتروني يتميز بالتحديث المستمر بصورة يومية، فيتم إنتاج فيروسات جديدة، تستغل الثغرات الحديثة التي تظهر في الأنظمة قبل أن يتم معالجتها.

الفرق بين الهجمات السيبرانية والجرائم السيبرانية، والحرب السيبرانية:

ليان الفرق بين الهجمات السيبرانية وغيرها بشكل أوضح، فمن المهم التمييز بينها وبين الجرائم السيبرانية والحرب السيبرانية:

1. فان التمييز بين الهجمات السيبرانية والجرائم السيبرانية، حيث تشترك الجرائم السيبرانية الهجمات السيبرانية في المجال التي تحدث فيه أي فضاء سيبراني، الا إنها تختلف عنها من ناحيتين:

أ. غالباً السيبرانية هم الافراد وتوجه ضد الناحية الأولى: بالنسبة للأشخاص ما يكون مرتكبي الجرائم مؤسسات مالية أو شركات وحتى أفراد داخل أو خارج إقليم الدولة، بخلاف الهجمات التي تتم من قبل دول (1) أو مجموعات حكومية أو غير حكومية ضد دولة أخرى

ب. يكون الهدف من الجرائم السيبرانية بالنسبة للأهداف: غالباً إثبات مهارة الفاعل تقنيا وقدرته على اختراق أجهزة الكمبيوتر أو تهدف التسلية والترفيه أو تحقيق مكاسب شخصية كسهرقة الملكية الفكرية عن جريقت شبكات الحاسب الآلي أو التسلل إلى أنظمة المصارف والتلاعب بأرقام الحسابات وتحويل الأموال دون الحاجة إلى تدمير وتعطيل شبكة الكمبيوتر المستهدفة (رغم أنه قد يعطلوها في بعض الجهات) وتكون هذه الأفعال مجرمة بموجب القانون الوطني، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي والسياسي للدولة ويقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية .

لماذا تمثل العمليات العسكرية السيبرانية شأغلاً إنسانياً؟

تحتل الهجمات السيبرانية وعواقبها مكان الصدارة على جداول الأعمال في جميع أنحاء العالم. وما يثير القلق هو أن العمليات العسكرية السيبرانية تتحول أيضاً

إلى جزء من النزاعات المسلحة اليوم، ويمكنها أن تعطل عمل البنية التحتية بالغلة الأهمية والخدمات الحيوية للسكان المدنيين.

ويزداد اعتماد نظم الرعاية الصحية على الرقمنة والاتصال بالإنترنت، ولكنها تفتقر إلى الحماية في غالب الأحيان، ولذلك، فهي معرضة بشكل خاص للهجمات السيبرانية. وفي كثير من الأحيان تتضرر البنية التحتية للمياه والطاقة، أو المستشفيات، في النزاعات المسلحة جراء القصف، وتعمل الخدمات جزئياً فقط أو لا تعمل على الإطلاق، ولك أن تتخيل أثر وقوع حادث سيراني كبير علاوة على هذا! فقد يترتب على ذلك عواقب وخيمة. ويكفي المدنيين العالقين في برائن النزاع والعنف ما يعانونه أصلاً حتى يروا صعوباتهم تتفاقم أكثر فأكثر.

ويتم الاعتماد بشكل متزايد على التكنولوجيات الجديدة والرقمية من أجل دعم البرامج الإنسانية، مثلاً عن طريق تسجيل المعلومات واستخدامها لتوجيهه وتكييف الاستجابات أو عن طريق تيسير التواصل بين الموظفين العاملين في المجال الإنساني والمدنيين المتضررين من النزاع أو العنف. ولكن هذا أيضاً يجعلنا عرضة للعمليات السيبرانية التي قد تؤثر على قدرتنا على توفير الحماية والمساعدة أثناء حالات الطوارئ الإنسانية. (اللجنة الدولية للصليب الأحمر، 2019)

ونلاحظ أيضاً تزايد خطر تعرض السكان المتضررين من النزاعات لضرر متعمد وغير متعمد، لا سيما من خلال (إساءة) استخدام البيانات من جانب الأطراف المتحاربة و/أو انتشار المعلومات المضللة والمعلومات الكاذبة وخطاب الكراهية.

وبينما أقر عدد ضئيل من الدول علناً باستخدام وسائل سيبرانية لدعم عملياتها العسكرية، تشير التقديرات إلى أن أكثر من 100 دولة قد طوّرت - أو تعمل على

تطوير - قدرات عسكرية سيبرانية. ولحسن الحظ، لا تحدث العمليات السيبرانية أثناء النزاعات المسلحة في ظل فراغ قانوني، إذ تخضع للقانون الدولي الإنساني.

القانون الدولي الإنساني وشرعية الحرب السيبرانية:

فالتأكيد على انطباق القانون الدولي الإنساني على العمليات السيبرانية أثناء النزاعات المسلحة لا يضيف الشرعية على الحرب السيبرانية، تماماً مثلما لا يضيف القانون الدولي الإنساني الشرعية على أي شكل آخر من أشكال الحرب.

وفي الواقع، أثير هذا الخوف من احتمال إضفاء الشرعية على الحرب مراراً في المناقشات الحكومية الدولية. ولكن الدول عالجت هذا الخوف في عام 1977 حين نصّت - في ديباجة البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949 - على أن القانون الدولي الإنساني يجب ألا "يفسر على أنه يجيز أو يضيف الشرعية على أي عمل من أعمال العدوان أو أي استخدام آخر للقوة يتعارض مع ميثاق الأمم المتحدة".

ويختلف القانون الدولي الإنساني عن ميثاق الأمم المتحدة، ولكنهما متكاملان. وعملياً، يحظر ميثاق الأمم المتحدة استخدام القوة إلا في حالة الدفاع عن النفس أو عندما يأذن مجلس الأمن التابع للأمم المتحدة بذلك. وهو يتطلب أيضاً تسوية النزاعات الدولية بالوسائل السلمية. ولكن، إذا نشب نزاع مسلح، ينطبق بعد ذلك القانون الدولي الإنساني لتوفير سبل الحماية الأساسية للأعيان المدنية والأشخاص (المدنيين) الذين لا يشاركون أو كفّوا عن المشاركة (مثل الجنود الجرحى أو المحتجزين) في الأعمال العدائية.

ولا يحل القانون الدولي الإنساني محل ميثاق الأمم المتحدة أو يستبعده، بل يضيف مستوى من الحماية لجميع ضحايا الحرب في الحالة المؤسفة التي تندلع فيها الحرب.

التمييز بين الأمان في الفضاء السيبراني والجرائم السيبرانية والأمن السيبراني.

قد لا تكون جميع الاعتداءات في الفضاء السيبراني مجرمة في القانون الجزائي في بعض الدول، وذلك غير ملائم بالرغم من الاضرار التي قد تنشأ عنها؛ وفي هذه الحالة، تعتبر المضايقات والهجمات الإلكترونية سلوك مالمم ويتطلب قواعد وخطط لأمان السيبراني **Plan Safety Cyber**، حيث يجري التركيز على المخاطر مجرمة جزائياً العريضة الشخصية والاجتماعية الناتجة عن استعمال الحاسوب، أما عندما تكون هذه الافعال فتعتبر هذه الهجمات والمضايقات السيبرانية جرائم سيبرانية وتتطلب خطة وطنية لمكافحة **National Cybercrime** **Combat plan** أما حين تتماهى الاعتداءات لتطال الأمن القومي، فنكون في صدد استراتيجية للأمن السيبراني **Strategy Security Cyber**، حيث يجري العمل على خطة لفضاء سيبراني آمن وموثوق، بحيث تكون الدولة قادرة على مجابهة الهجمات على البيانات والأنظمة، ولا سيما الهجمات التي تطال البنية الاساسية الحساسة والأنظمة المعلوماتية للأمن القومي، ويمكن القول إن العمل على توفير الامان والأمن في الفضاء حكماً يساهمان في مجابهة الجرائم.

الفصل الخامس

الجهود الدولية، والتنظيم الدولي

مُكافحة الهجمات السيبرانية

من المؤكد أن إدخال أي تكنولوجيا جديدة يؤدي إلى ظهور تحديات قانونية جديدة. غير أنه من الممكن مع التطور التكنولوجي المعلوماتي تطبيق التشريعات التقليدية التي تركز على الأشياء الملموسة ضمن حدود معينة، على أن يصاحبها صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والأنظمة المعلوماتية، حيث يصعب تحديد صاحب أو حائز المعلومة، ولا سيما على صعيد التجريم والاختصاص القضائي وإجراءات التحقيق والدلة المعلوماتية. ومع العلم أن النوع الثاني من الجرائم السيبرانية يخضع تجريمها بنصوص خاصة للنصوص العامة أيضا للنصوص العامة وللنظرية العامة لقانون العقوبات فيما يتعلق بتحديد أركان الجريمة والمشتكرين والمحاولة الجرمية وأسباب الدفاع المشروع وغيرها.

ويبدو أن معظم الدول تحاول توسيع نطاق تطبيق تشريعاتها التقليدية لتشمل الفضاء السيبراني والجرائم السيبرانية، وعلى صعيد الدول العربية، يجهد القضاء لمحاولة تطبيق نصوص قانون العقوبات التقليدي على الجرائم السيبرانية لتدارك النقص في التشريعات السيبراني.

ويبدو أن دول عديدة في العالم مازالت تعمل على تحديث تشريعاتها في الجانب الموضوعي وكذلك في الجانب الاجرائي، وذلك لضمان محاربة الجرائم السيبرانية. فبعض الظواهر الإجرامية ازدادت وتعاضمت الاضرار الجرمية الناتجة عنها، وأصبح من المفترض إعداد تشريعات خاصة لتجريمها. وهذه الظواهر تتمثل بالبريد غير المرغوب فيه (spam) وسرقة الهوية، وتجريم الافعال التحضيرية، وليس فقط في المحاولات الجرمية والهجمات السيبرانية المنسقة والهائلة ضد البنية الاساسية الحساسة وغيرها. وقد أضيفت إلى الجرائم السيبرانية الجرائم الخاصة بالعنف ضد المرأة والمطاردة والمضايقة على الفضاء السيبراني.

المبحث الأول: الجهود الدولية في مجال مكافحة الإرهاب السيبراني

للفضاء السيبراني في عصر العولمة دور مهم في جميع ميادين الحياة، فقد جعل من العالم قرية صغيرة وبسببه نمت مخاطر و تهديدات باتت تهدد دوره وأهميته الإستراتيجية بعد التحول الرئيسي الذي ظهر في سياسات الأمن والدفاع مع انتهاء فترة الحرب الباردة، بحيث كان الأمن خلال تلك الفترة مضامين معينة، ثم جاءت ثورة المعلومات والتكنولوجيا أضيف إليها ملامح وأبعاد أخرى جديدة، ومع بداية سنوات التسعينيات من القرن الماضي، بدأت موجة الانتشار الدولي لتكنولوجيا والاتصال والمعلومات، لتتدخل في مختلف ميادين الحياة السياسية والإجتماعية والأمنية والاقتصادية وغيرها.

وفي الوقت نفسه، تعرضت الوسائل التكنولوجية الجديدة للإستعمال الخطير من قبل التنظيمات الإرهابية التي استفادت بشكل كبير من التسهيلات التي أتي بها المجال السيبراني باعتباره أحد المحددات الجديدة للقوة، وبالنظر إلى الأبعاد الجديدة التي تنطوي عليها القوة الإلكترونية من حيث طبيعتها وأنماط وهو ما شك تأثيرات كبيرة وعميقة على قدرات الدول وعلاقاتها استعمالها، بل وأيضاً طبيعة الفاعلين، الخارجية ومجموعة وسائلها وطاقاتها ومكانياتها المادية وغير المادية، المنظورة وغير المنظورة، والتي يستخدمها صانع القرار في تحقيق مصالح الدولة والتأثير في سلوك الوحدات السياسية الأخرى.

لقد أدت البيئة التكنولوجية مع انتشار تكنولوجيا الاتصال والمعلومات وارتباطها بأعمال المال سعت والاقتصاد والمجتمع الدولي، حتى أصبح الأمن السيبراني تحدياً يندرج ضمن أجندات الأمن الوطني للدول خاصة مع علاقته بالإرهاب وحماية البنية

التحتية، وفي ذات الأثناء، ظهرت قطاعات حديثة في الاقتصاد تعتمد على التكنولوجيا المعلوماتية، وأصبح الأمن السبيري أكبر اعتماداً مُهم يمثل عنصر عناصر الأمن الوطني واستراتيجياته، بالنظر إلى أهمية الفضاء السبيري في تطور الاقتصاديات الحديثة.

إن الخطورة التي تكمن فقط في تعرض أنظمة المعلومات للفشل، بل أيضا في أنها أصبحت أهدافاً للهجمات التي تؤثر بدورها على عمل البنية التحتية الكونية للمعلومات والخدمات المتقدمة التي هي محتملة للتعرض للهجمات، وما لذلك من آثار اقتصادية وسياسية واجتماعية وأمنية كبيرة، وما يزيد حجم المعضلة أن تلك الهجمات قد حد تكون صغيرة ورخيصة، ولكنها اثراً ضخمة من خلال شبكات المعلومات والاتصال الإرهاب السبيري والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة لذا أصبحت التهديدات الجديدة تستحوذ على اهتمام متزايد من العديد من الدول، خاصة تلك التي ترتبط بالتكنولوجيا والمتقدمة صناعيا، إذ يهتم بها صانعو القرار، وتقع ضمن أولويات الاجندة الأمنية والسياسية، وتعود أولى الجهود الدولية لمواجهة الجريمة السبيرية والإرهاب الرقمي إلى ثلاثة عقود مضت، حين ناقش الانتربول الدولي في عام 1821 إمكانية إيجاد تشريع قانوني خاص بالجريمة الإلكترونية.

وقد كان التقدم بطيئا، لكنه أخذ في التسارع المطرد بعد انتهاء الحرب الباردة، ولعل إنشاء معهد قانون الفضاء السبيري في جامعة جورج تاون الأمريكية عام 1881م يدل على نمط المشكلة، بحيث فيه تواجد ثلاثون متخصصا من الذين يعملون على كيفية التعامل مع مشكلات الفضاء السبيري، وأمام التحديات المطروحة، جدت وثلاث استراتيجيات لحماية البنية التحتية للمعلومات في الولايات

المتحدة الأمريكية تتضمن: الفعل العسكري "التدخل"، الحلول الفنية لتأمين الأنظمة والاستعداد وبناء الوعي "المعلومات". في حين جاءت السياسات الحكومية الخاصة بمكافحة هجمات ض الفضاء السيبراني وتعزيز الأمن السيبراني متنوعة في مراحل تنفيذها، بعدها كان قويا، بينما كانت الاخرى مجرد اقتراحات، وجاءت بأشكال وصور متنوعة من بينها اتباع سياسة تنظيمية خاصة بالبنية التحتية للمعلومات لتضمن الاجراءات الخاصة بالأمن السيبراني في الجهود العامة لمكافحة الإرهاب.

لقد أخذ الاهتمام بالأمن السيبراني في الانتشار على المستوى الدولي، وخاصة داخل الدول المتقدمة، وظهر ذلك في تبني سياسات أمنية متعددة، وسعت العديد من الدول العالم خلال سنوات قليلة إلى زيادة الاهتمام بهذه الظاهرة، رغبة في تأمين نظم المعلومات التي أصبحت تهدد النمو الاقتصادي والأمن الوطني والدولي .

وقد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني والثنائي والاقليمي والدولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة في إطار صياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدولي. وقد فرض ذلك الحاجة إلى تحديد ما يمكن أن يمثل بنية تحتية حرجية، في ظل تبني إجراءات قانونية وأمنية صارمة بإمكانها الوقاية والتصدي للتهديدات ذات الخصائص غير التقليدية كحال الإرهاب الإلكتروني .

وقد عكست الجهود الدولية في مجال الأمن السيبراني اهتماماً واضحاً ومتزايداً من جانب القطاعين الخاص والعام أو بالتعاون فيما بينهما، كما سعى العديد من البلدان المتقدمة إلى تبني استراتيجية دولية في مجال تأمين الفضاء السيبراني، من

خلال جملة من القوانين وأهمها مبادرة الشراكة الدولية المتعددة الأطراف لمكافحة الإرهاب السيبراني، التي تهدف إلى حشد الجهود الدولية لمكافحة الإرهاب السيبراني والتهديدات العالمية الجديدة وأساليب المواجهة من جانب القطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهة التهديدات المتزايدة التي يمثلها الإرهاب السيبراني، كما سعت المبادرة إلى جمع الرؤى والأفكار حول التدريب وتبادل الخبرات، وتم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الرقمي وحماية الأمن السيبراني وكانت تلك المواقع نقطة التقاء بالنسبة لخبراء أمن المعلومات والسياسيين من أجل التباح حول ماهية خطر الإرهاب السيبراني وكيفية مواجهته، مثل مجموعة "SITE" للاستخبارات، التي تعد جهاز استخبارات متخصصا في رصد الإرهاب عبر الإنترنت ودراسة المصادر الأولية للارهابيين والمرجعيات الفكرية لهم وترجمة أحاديثهم، ومراقبة دعاية الإرهابيين.

المبحث الثاني: التنظيم الدولي لمكافحة الهجمات السيبرانية

يتضمن التنظيم الدولي لمكافحة الهجمات السيبرانية عدة نواحي تمثل فيما يلي:

التعاون الدولي بين أجهزة الشرطة:

لقد أدى التطور الكبير في وسائل المواصلات بصفة عامة والشبكة المعلوماتية بصفة خاصة إلى انتقال المجرمين من بلد إلى آخر، وقد أدرك المجتمع الدولي أنه بات من المستحيل على أي دولة أن تقوم بالقضاء على الجرائم العابرة للحدود، ذلك أن الإجراءات العامة لأجهزة الشرطة في كل دولة لا تجعل لجهازها الأمني تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، وعليه فإن الحاجة إلى تعاون أجهزة الشرطة فيما بين الدول وتنسيق العمل فيما بينهم لمطاردة المجرمين، ومن أبرز مظاهر التعاون أنشاء منظمة الشرطة الجنائية الدولية "الإنتربول" وظهور العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة، وتتمثل هذه الصور والوسائل فيما يلي:

ربط شبكات الاتصال والمعلومات:

يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين تلك الأجهزة في الدول الأخرى عن طريق السلك الدبلوماسي، خاصة إن الاتصالات الشرطية تحتاج إلى عملية اتصالات خاصة تحقق لها السرعة المطلوبة؛ لذا حاولت المنظمة الدولية للشرطة الجنائية "الإنتربول"، وكذلك العديد من الدول تطوير نظم الاتصال وتبادل المعلومات فيما بينها، حتى يتم الوصول وتعقب المجرمين بمجرد خروجهم من الدولة التي تم ارتكاب الجريمة فيها فتقوم أجهزة شرطة الدولة

المجنبي عليها بالاتصال السريع بالأجهزة الأمنية في الدولة المتفق معها أمنيا للقيام بملاحقة المجرمين في حدود دولتهم التي هرب إليها. (بن داود، 2017)

المنظمة الدولية للشرطة الجنائية "الانتربول":

ويُعد الانتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة، فمهمة الانتربول الاساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الاعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال التنسيق الشرطي العالي الحرفية وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسلمهم إلى الدولة التي تطلب تسلمهم، وإنشاء وتطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام. (الزهراني، 2020)

هذا ويعهد بتلك المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو وإلى جهاز دائم يتم تعيينه بواسطة السلطات الحكومية الوطنية، وبمساعدة فرق الانتربول للتحرك إزاء الاحداث التي يمكنها تيسير مجموعة من خدمات التحقيق والتحليل في موقع الحدث بالتنسيق مع الامانة العامة، ويقوم الانتربول بتعميم التحذيرات والتنبيهات المتضمنة المعلومات الإستخبارية والاحاطات الهامة والمشورة التحليلية والفنية عن الأخطار الإجرامية المحتملة، ويستخدم الانتربول أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها والتقصي في قواعد البيانات وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم الإنترنت، من خلال الاستعانة

بمجموعة من الخبراء الدوليين والمُختبرات الدولية على الصعيد العالمي وتيسير تبادل وتحليل وتخزين البيانات الجنائية حيث تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الإنترنت وكيفية التدريب على مكافحتها والتحقيق فيها، ويعد الإجرام المالي المرتبط بالتكنولوجيا المتقدمة من الجرائم التي تركز عليها منظمة الإنترنتبول. (العازمي، 2016)

تبادل التعاون لمواجهة الكوارث والأزمات:

في حالة وجود أزمة وفي المواقف الحرجة، فإن عنصر الوقت يعد من الأمور الحاسمة في مواجهة تلك الأزمة أو الكارثة، الأمر الذي يحتاج معه إلى تكثيف وزيادة الجهود والخبرات وإلإمكانيات وهو ما لا يمكن تحقيقه الا بتركيز الجهود الدولية في مسار واحد، فعلى سبيل المثال: مشاركة قوات الانقاذ والدفاع المدني للدول المنكوبة اثر الزلازل والأعاصير والفيضانات أو المشاركة بخبراء أو تقديم معدات متطورة، كذلك المشاركة بقوات خاصة أو خبراء، أو تجهيزات في تحرير رهائن محتجزين، أو مباني هامة محتلة أو طائرات، أو سفن مُختطفة. (يوسف، 2011)

القيام بالعمليات الشرطية الدولية المشتركة:

تتمثل العمليات الشرطية كالتسليم المراقب في مجال مكافحة المخدرات، فهو يعني السماح لشحنة غير مشروعة بالمرور تحت المراقبة عبر إقليم ما، وكذلك المطاردات الساخنة والتي يقصد بها تعقب الجناة الذي يبدأ في احدى الدول ويواصل في أراضي دولة أخرى.

مظاهر التعاون الشرطي الدولي في مجال مكافحة الهجمات السيبرانية:

شرطة الويب الدولية:

أنشئت هذه المنظمة في الولايات المتحدة الأمريكية عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقرصنة إلكترونياً والبحث عن الأدلة ضدهم، وتقديمهم للمحاكمة، ويضم فريق العمل بهذه المنظمة متخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من 61 دولة حول العالم، ونظراً لاتساع نشاط هذه المنظمة وما تقوم به من إجراءات بالتعاون مع وكالات إنفاذ القانون في الدول الأعضاء فإن ذلك يسهل الأمر لفريق العمل بتتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم، وفي إطار مسألة الضوابط القانونية التي تحكم حركة مرور المعلومات عبر شبكة الإنترنت.

فهناك من يرى أنه من الضروري وضع ضوابط وقواعد بحيث لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان من ناحية، ولا تستخدم الشبكة لأغراض إجرامية أو نشر مواد إباحية تسيء إلى المجتمع من ناحية أخرى وإن الإشكالية ليست في حجب الصور والمواقع الإباحية، بل من الكثير من ذلك المواقع التي تبث أفكار تفسد المجتمع والتي تدعو إلى التظاهرات أو الانقلابات تحت ما يسمى بالحريات العامة وحقوق الإنسان فحق المجتمع في الاستقرار والتقدم والرفق أهم بكثير من النظر إلى حق الفرد أو المصلحة الخاصة، إلا إن الصعوبة التي تواجه أجهزة شرطة الإنترنت عندما تنفذ الجريمة من خلال مقاهي الإنترنت، ففيها يقوم العملاء

بتنفيذ ما يريدون من جرائم دون إمكانية تحديدهم، حيث لا تتطلب هذه المقاهي من زبائنها إثبات شخصيتهم. (الزهراني، 2020)

ومثال على ذلك إن المباحث الفدرالية بالولايات المتحدة بعد أن تتبع أحد القراصنة، والذي اخترق شبكة معلومات أحد المصارف إلا أنها لم تستطع تحديده ومحاكمته؛ إلا أنه تبين أنه نفذ عملياته من خلال عدة مقاهي للإنترنت، ولحل تلك الإشكالية فإنه يجب على الدول إلزام أصحاب مقاهي الإنترنت بإثبات شخصيات رواد المقهى قبل الدخول بالإضافة إلى وجود كاميرات مراقبة تبين بوضوح تفاصيل وجه جميع رواد المقهى ولا يعتمد على إثبات الشخصية فقط لأنه من الممكن أن تكون البيانات الواردة في تحقيق الشخصية مزورة، فتقوم الكاميرات بتحديد شخص المستخدم، وذلك بهدف تلقي البلاغات وتتبع الجرائم والاحتياالات التي ترتكب من خال شبكة الإنترنت بالتنسيق مع أجهزة المكافحة والضبط المعنية داخل الولايات المتحدة الأمريكية وخارجها من خلال موقع المركز على الشبكة الدولية، ومن أجل إحكام الرقابة على شبكة الإنترنت فقد طبقت دولة الامارات العربية المتحدة ما يعرف بنظام الرقيب الذي يقوم بمراجعة نوعية الخدمات المقدمة عبر شبكة الإنترنت، فعندما يطلب المشترك موقعاً على الشبكة الأم تصل الإشارة إلى الرقيب الذي يقوم بدوره بعرض الموضوع على قائمة كبيرة جداً من المواقع الممنوعة.

(الزهراني، 2020)

تعاون السلطات القضائية للدول:

يوازن التعاون القضائي الدولي بين إستقلال الدولة في ممارسة اختصاصها الجنائي على حدود إقليمها وبين ضرورة ممارسة حقها في العقاب، فبدون هذا التعاون فلا يمكن للدولة من الناحية العملية إقرار حقها في العقاب وعلى ذلك فابعد من التعاون الدولي لسببين: (الزهراني، 202)

1. إن الدولة تتقيد بحدودها الإقليمية، فقانون العقوبات يمكن أن يتعدى نطاق تطبيقه إلى ما يجاوز حدود إقليم الدولة، إلا أنه لا يمكن مباشرة الإجراءات خارج الإقليم الوطني لا ممارستها تمس سيادة الدول الأجنبية الأخرى .

2. لا يمكن تطبيق قانون العقوبات بدون قانون الإجراءات الجزائية، فالإجراءات الجزائية هي الوسيلة اللازمة لتطبيق قانون العقوبات ونقله من حالة السكون إلى الحركة، وعلى ذلك فإنه إذا تطلب تطبيق قانون العقوبات مباشرة بعض الإجراءات الجزائية خارج حدود إقليم الدولة فإنه يجب عدم الاصطدام بمشكلة الحدود الإقليمية بين الدول، ووجب الالتجاء إلى التعاون القضائي لتذليل هذه الصعوبة، ويتمثل هذا التعاون في مجموعة من الوسائل التي بواسطتها تقدم إحدى الدول المعاونة سلطاتها العامة، أو مؤسساتها القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى.

وحيث إن جرائم الإنترنت ذات طابع عالمي وبالتالي يمكن أن تتعدى آثارها عدة دول؛ فإن ملاحقة مُرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرائية خارج حدود الدولة، مثل

المعاينة، أو ضبط الاقراص الصلبة التي توجد عليها معلومات غير مشروعة أو تفتيش الوحدات الطرفية في حالة الاتصال عن بعد أو القبض على المتهمين أو سماع الشهود أو اللجوء إلى الانابة القضائية أو تقديم المعلومات التي يمكن أن تسهم في تحقيق الجرائم، فكل ذلك لن يتحقق الا بمساعدة الدول الاخرى.

وتتخذ المساعدة القضائية عدة صور هي:

1. تبادل المعلومات:

يتمثل ذلك في تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما أن هناك مظهر آخر من مظاهر تبادل المعلومات وهو ما يتعلق بالسوابق القضائية للجنة من خلالها تتعرف الجهة القضائية بدقة على الماضي الجنائي للفرد المحال إليها، فهي التي تساعد في تطبيق الاحكام الخاصة بالعود ووقف تنفيذ العقوبة وعدم الاهلية .

2. نقل الاجراءات: (الزهراني، 2020)

يقصد بنقل الإجراءات قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك إذا توافرت الشروط التالية:

أ. أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.

ب. يجوز ألي طرف متعاقد ان يطلب من أي طرف آخر أن يتخذ الإجراءات الجزائية في أي حالة من الحالات الآتية :

✓ إذا كان الشخص المتهم خاضعاً أو سيخضع لحكم يقيد الحرية في الدولة الطالبة. إذا كانت الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.

✓ أن يكون الاجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة الموجودة بالدولة المطلوب إليها إذا كان تنفيذ الحكم في الدولة المطلوب إليها يحقق إعادة التأهيل الاجتماعي للشخص المحكوم عليه.

✓ إذا كان حضور الشخص المتهم في الجلسة لا يمكن ضمانه في الدولة الطالبة بينما يتحقق ضمان حضوره في الدولة المطلوب إليها ويجوز للدولة المطلوب إليها أن ترفض نقل الاجراءات في الحالات الآتية: (الأوجلي، 1997)

أ. إذا كان طلب نقل الإجراءات ليس له ما يبرره بأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذه الإجراءات.

ب. إذا ثبت أن الباعث من وراء طلب نقل الإجراءات اعتبارات عنصرية أو دينية أو سياسية، إذا كانت الدولة المطلوب إليها قد طبقت قانونها على الجريمة قبل استلامه من الدولة الطالبة وكان الاجراء الذي سبق اتخاذه مطابقاً للقانون.

ت. إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات ملتزمة بها الدولة المطلوب إليها إذا كانت الاجراءات المطلوبة مخالفة للمبادئ الاساسية للنظام القانوني في الدولة المطلوب إليها الا ان هناك رأي يرى،

أن تطبيق هذه الآليات التقليدية من الاتفاقيات يثير بعض المشاكل، مثل وجود عقبات خاصة بالجرائم التي ترتكب عبر شبكة الإنترنت وأن كانت تلك العقبات موجودة على المستوى المحلي أو الوطني إلا أنها تثار أيضا على المستوى الدولي ومن بين هذه العقبات، تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق الدولي وإقامة الدليل على الجرائم التي ترتكب في مجال الإنترنت وذلك بالنظر إلى الاختلافات التي توجد بين التشريعات المختلفة فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود ووقف بث الرسائل ذات المحتوى غير المشروع. (الزهراني، 2020)

الإنابة القضائية الدولية:

تعد الإنابة القضائية إحدى صور المساعدة القضائية للتعاون العقابي الدولي، فهي تجعل دولة ما تتمكن من الاستفادة من السلطات العامة لدولة أخرى إذا ما حالت الحدود، ويقصد بالإنابة القضائية الدولية، طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به دولة الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، وعلى ذلك فالإنابة القضائية هي إجراء لتسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل إقليم الدول الأخرى . (السند، 2011)

ومن أمثلة ذلك سماع الشهود وإجراءات السير في الدعوى الجزائية، وتتم الانابة القضائية بين الدول عن طريق الاتفاقيات والتي تتضمن شروط وأساليب تنفيذ الانابة القضائية، وغالبا ما تتضمن شرط باستبعاد تنفيذ الاحكام في المجال السياسي والضريبي والعسكري، أو اذا قدرت الدولة المطلوب منها ان التنفيذ المطلوب من شأنه المساس بسيادة الدولة أو النظام العام أو المصالح الاساسية الأمر الذي يترك للدولة سلطة تقديرية لتنفيذ أو عدم تنفيذ ما يطلب منها وذلك خشية قيام مسؤوليتها دوليًا عن إهمالها، وفي ظل عدم وجود اتفاقية فإن الانابة القضائية لا يمكن تنفيذها الا إذا وافقت الدولة المطلوب إليها على ذلك وفقا للاجراءات والشروط المنصوص عليها في القانون الداخلي لها. (الزهراني، 2020)

الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني:

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة، ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية مُعاهدة بودابست لمكافحة جرائم الإنترنت وتوصيات المجلس الاوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات والتي هي:

أ. توصيات المجلس الاوروبي:

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى

إصدار المجلس الأوروبي التوصية رقم 95/13 في 11/9/1995 بشأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الاعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتواءم من التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي: (رمضان، 2000)

1. أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.
2. أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلاً للتفتيش مع بيان المعلومات التي تم ضبطها، ويسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش .
3. أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الاجراء ضروريا.
4. أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

5. تطبيق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية و الاحترام للمعلومات التي يفرض القانون لها حماية خاصة.
6. إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الإتصال بالتعاون مع سلطة التحقيق لاجراء المراقبة و التسجيل.
7. يتعين تعديل القوانين الاجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
8. يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ الاجراءات اللازمة للسماح لرجال التحقيق بالاطلاع عليها، وأن تخول سلطات التحقيق بإصدار أوامر مماثلة إلى شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.
9. تطوير و توحيد أنظمة التعامل مع الادلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الاجرائية الخاصة بالادلة التقليدية على الادلة الإلكترونية.
10. تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

11. قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الاجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الاجراءات .

12. أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة، ويتعين عندئذ ان تسمح السلطة الاخيرة بإجراءات التفتيش والضبط، ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة.

3. معاهدة بودابست لمكافحة جرائم الإنترنت:

تُعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست في 2003/11/23، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت الاستخدام السيء لها، وقد وقعت على تلك المعاهدة 26 دولة أوروبية، بالإضافة إلى كندا واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام، وتتضمن 48 مادة على أربعة فصول هي الآتية وتعريفات خاصة ببعض التعريفات الفنية الفصل الثاني يتضمن

الإجراءات الزم اتخاذها على المستوى المحلي لكل دولة، وتنقسم إلى قسمين: (الجهيني، 2004)

القسم الأول: يتعلق بالنصوص الجنائية الموضوعية على النحو التالي:

أ. بشأن الجرائم ضد الخصوصية وسامة وتواجد معلومات الحاسب ونظم الحاسب ويشمل وصفاً لأنواع متعددة من الجرائم.

ب. الجرائم المتصلة بالحاسب شاملة استخدام الكمبيوتر في التزوير والأفعال الاحتيالية.

ت. الجرائم المتعلقة بالمحتوى والمضمون.

ث. الجرائم المتصلة بالتعدي على حقوق المؤلف.

القسم الثاني: القانون الاجرائي فيما يتصل بالإجراءات الجنائية شاملة الحفاظ على المعلومات المخزنة والأوامر الخاصة بتسليم الأدلة، وتتضمن كذلك تفتيش وضبط بيانات الحاسب المخزنة.

التعاون الدولي وتسليم الجناة والمساعدة المشتركة:

لقد حددت المعاهدة الدولية الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان، ومزودي خدمات الإنترنت من قلق حيث تخشى منظمات حقوق الإنسان من أن تحد المعاهدة من حرية الأفراد، وأن تؤدي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت.

تسليم المتهمين للعدالة:

أدى سهولة هروب المتهمون من الخضوع للعقوبة في الجرائم السيبرانية، وتعذر وصعوبة الملاحقة بهم إلى ضرورة لجوء الدول إلى طريق التسليم، وتتبع المجرم حيثما كان لكي لا يفلت من العقاب وبالتالي مكافحة الجريمة السيبرانية وحماية المجتمعات من المخيلين بأمنها واستقرارها على المستوى الدولي والمحلي، وحتى لا يظل هؤلاء المجرمون بمأمن من العقاب، يفعلون ما يشاءون، وفي نطاق حديثنا عن نظام تسليم المتهمين سوف نقوم بالحديث عن مفهوم هذا النظام، وشروطه وإجراءاته بوجه عام، ثم نستتبع ذلك بالحديث عن نظام تسليم المتهمين في مجال الجرائم السيبرانية وذلك على النحو التالي (الزهراني، 2020):

مفهوم نظام تسليم المتهمين:

نظام تسليم المتهمين هو "إجراء تعاون دولي تقوم بمقتضاه دولة تسمى بالدولة المطلوب إليها بتسليم شخص يوجد في إقليمها إلى دولة ثانية تسمى بالدولة الطالبة أو جهة قضائية دولية، بهدف ملاحقة عن جريمة اتهم بارتكابها أو الرجل تنفيذ حكم جنائي صدر ضده، وعليه فإن فكرة تسليم المتهمين تقوم من ناحية على وجود علاقة بين دولتين، الدولة الأولى تطالب بأن تسلم إليها مُرتكب الجريمة لتتخذ بحقه الإجراءات الإلزامية، والدولة الثانية يوجه إليها طلب التسليم لتقرر بعد ذلك إما الاستجابة له إذا كان متوافقاً مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق بين البلدين، وإما الرفض لعدم وجود ذلك التشريع أو تلك الاتفاقية، ومن ناحية أخرى نجده يشمل طائفتين

من الأشخاص، الطائفة الأولى هم طائفة الأشخاص المتهمين الذين تسند اليهم تهمة ارتكاب جرائم الا أنه لم يصدر بحقهم أية أحكام قضائية بعد والطائفة الثانية، هو الأشخاص المحكوم عليهم الذين صدر بحقهم حكم التسليم على ثلاثة قضائي بالادانة الا أنه لم ينفذ بعد نتيجة فرارهم إلى دولة أخرى.

إذ أن أنواع التسليم متعدد وتشمل تسليم إداري وتسليم قضائي، وتسليم مختلط: وهناك شروط نظام تسليم المتهمين ثاني وهناك شروط لا بد من توافرها حتى يتم العمل بنظام تسليم المتهمين، وتتمثل أهمية تلك الشروط في كونها تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم وتضع الاحكام العامة التي على أساسها سيتم التسليم من عدمه، وإذا توافرت هذه الشروط يتم البت في قرار التسليم.

وتكاد تتفق هذه الشروط في جميع حالات التسليم من حيث العناصر، أما من حيث الموضوع فهي محل خاف بين الدول وذلك على حسب حاجتها للتسليم واعتبارات المصالح الدولية التي تراعيها كل دولة و تتمثل هذه الشروط فيما يلي:

أ. شرط ازدواج التجريم: يقصد بهذا الشرط أن يكون الفعل المطلوب التسليم من أجله مجرماً في تشريع كل من الدولتين الطالبة والمطلوب إليها التسليم، والمطلوب هنا أن يكون الفعل مجرماً أيأ كانت الصورة التشريعية المعاقب عليها، فالعبرة للوصف، أو التكييف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، فقد تختلف تشريعات الدول في التكييف القانوني الذي توصف فيه

الجريمة فعلى سبيل المثال لو كان الفعل معاقبا عليه في تشريع الدولة طالبة تحت مسمى جريمة توظيف الاموال، بينما كان الفعل نفسه معاقبا عليه تحت مسمى النصب والاحتيال في الدولة المطلوب منها التسليم، فان ذلك لا يمنع من توافر شرط ثنائية التجريم أو ازدواجيته. (الأوجلي، 1997)

ب. شرط التجريم المزدوج يجد أساسه في أن الدولة طالبة التسليم تريد من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي، أو تنفيذ العقوبة المحكوم بها عليه، وهذا يفترض بداهة ان السلوك مجرم في تشريعها، إذ إنه إذا لم يكن مجرما فيتصور وجود دعوى جنائية أو ملاحقة جزائية ضد شخص المتهم، كما لا يتصور قيام حكم جزائي يقضي بالعقوبة عليه، هذا من جهة، ومن جهة أخرى لا يجوز مطالبة الدولة المطلوب منها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الاصل غير مجرم وفقا لقانونها، ويذهب أغلب الفقه .

إن شرط ازدواج التجريم قد يكون عقبة في مجال تسليم المجرمين، ففي التشريعات الجنائية الوطنية نجد أن الجرائم المعلوماتية غير معاقب عليها في معظم الدول هذا من جهة ومن جهة أخرى انه من الصعب تحديد ما إذا كانت النصوص التقليدية في تشريعات الدولة المطلوب إليها التسليم يمكن أن تطبق على جرائم شبكات الحاسبات الالية والإنترنت أم لا تطبق، بمعنى آخر أنه من الصعب البحث في تشريعات الدول المطلوب إليها التسليم، وعما اذا كانت تشريعاتها الجنائية التقليدية يمكن ان تطبق على الجرائم المعلوماتية من عدمه وبالتالي يتوافر شرط ازدواج التجريم ام لا، بالاضافة إلى

أن الدول قد تفسر بتوسع شرط ازدواج التجريم، الأمر الذي يترتب معه إعاقة تطبيق الاتفاقيات الدولية في مجال تسليم المتهمين ويحول ذلك دون جمع الأدلة ومحاكمة مرتكبي جرائم الإنترنت، لذلك يجب أن يكون هناك تنسيق أو توحيد بين التشريعات المختلفة فيما يتعلق بتعريف الجرائم المعلوماتية وجرائم الإنترنت أو على الأقل عدم اشتراط ازدواج التجريم، وذلك كما جاء في الاتفاقية المبرمة بين كندا وأمريكا فيما تتعلق بالمساعدة القانونية المتبادلة التي لم تتطلب ازدواج التجريم كشرط للتعاون القضائي فيما بينهما وتدخل جرائم الإنترنت في إطار هذه الاتفاقية.(الزهراني،2020)

أهمية الأمن السيبراني في الأردن:

لا شك اننا اصبحنا نعيش في عالم تهيمن عليه احدث التقنيات الحديثة والتطور الكبير في قطاع الاتصالات وتكنولوجيا المعلومات الأمر الذي يتطلب التركيز والعمل على بناء مهارات جديدة للمستقبل الرقمي من خلال التدريب المتخصص في مجالات الذكاء الاصطناعي والأمن السيبراني، والتقنيات الحديثة للاتصالات المتحركة وإنترنت الأشياء، وغيرها من المجالات التي يتطلبها التحول الرقمي مما يسهم في ايجاد فرص عمل جديدة ويعزز ريادة الأعمال والتجارة الإلكترونية .

وقد رافق هذا التطور ما يعرف بالهجمات الإلكترونية او السطو الإلكتروني على المعلومات التي تعتبر عصب الدول بمؤسساتها وكذلك افرادها، فكان لا بد من تحصين هذه المعلومات والشبكات الحاسوبية من الاعتداءات، لذا كان الرادع لهذا النوع من الحرب هو تحقيق ما يسمى بالأمن السيبراني .

ويعد الأمن السيبراني في الأردن حديث العهد حيث نظم المشرع الأردني قانون الأمن السيبراني في الأردن عام 2019 وأتت الإرادة الملكية السامية بالموافقة على قانون الأمن السيبراني في شهر ايلول من نفس العام فيما صدرت الإرادة الملكية السامية بالموافقة على نظام المركز الوطني للأمن السيبراني في شهر كانون ثاني من عام 2020 .

ويهدف قانون الأمن السيبراني في الأردن لما يلي:-

- 1 - حماية المملكة من تهديدات حوادث الأمن السيبراني .
- 2 - بناء قدرات وطنية تضمن مواجهة التهديدات التي تعترض أنظمة المعلومات والبنى التحتية .
- 3 - خلق بيئة آمنة وجاذبة للاستثمار ومحفزة للأقتصاد الوطني.
- 4 - مراقبة الفضاء السيبراني الوطني وتوثيق حوادث الأمن السيبراني في الأردن .
- 5 - ايجاد جهة مرجعية تتولى تطبيق وتنفيذ السياسات العامة التي تنبثق عن الاستراتيجية الوطنية للأمن السيبراني .
- 6 - رفع مستوى الأمن الوطني العام والشامل للمؤسسات والأفراد .
- 7 - تطوير قدرات ردع ومراقبة وإنذار والاستجابة لحوادث الأمن السيبراني والتخفيف من الأضرار الناجمة عنها .
- 8 - حماية الأردن من أي هجمات محتملة قد تعترض أنظمة المعلومات في المستقبل .
- 9 - تهيئة جيل قادر على احداث التغيرات في ظل التسارع التكنولوجي الذي نعيشه .

ويعد تخصص الأمن السيبراني من التخصصات الجديدة في الجامعات الأردنية حيث دخل في الجامعات بداية عام 2019، حيث أولى الأردن اهتماما كبيرا بدراسة تخصص الأمن السيبراني في الجامعات من خلال توفيره للطلاب والطالبات الراغبين بالالتحاق بهذا التخصص، من أجل منحهم مجموعة من المعارف والتقنيات التي تمكنهم من فهم أساسيات أجهزة الحاسب الآلي، ونظم الأمان والحوسبة، وذلك لحماية البيانات والأنظمة من الاختراق، ومن أجل اكساب الطلبة المعرفة والمهارات والسلوكيات اللازمة لتحليل مشاكل الأمن السيبراني وتصميم الحلول المناسبة من خلال أفضل الممارسات، وتعزيز القدرة على الابتكار والريادة مع الالتزام بالأطر المهني والقانوني والأخلاقي والعمل بفاعلية ضمن فرق عمل متعددة الاختصاصات، كما يتم دراسة كيفية التصدي للهجمات الإلكترونية المختلفة والقرصنة مع فهم نظم الحوسبة، والعمل أيضا على الدمج بين الجانب النظري والجانب العملي لتدريب الطلبة على ممارسة تلك المهارات قبل التخرج لضمان مستوى الكفاءة والقدرة على خوض سوق العمل فور التخرج من أجل خلق جيل مبدع من الشباب ليسهم في حركة التنمية والازدهار في الأردن.

ويختلف دراسة الأمن السيبراني من جامعة إلى أخرى إلا أنها تتشابه فيما بينها في منح الطلاب الجامعيين مجموعة من المعارف والتقنيات التي تمكنهم من فهم أساسيات أجهزة الكمبيوتر ونظم الأمان والحوسبة من أجل حماية البيانات والأنظمة من الاختراق. (الدستور 2022 م)

فرص العمل لتخصص الأمن السيبراني في الأردن:

إن مستقبل سوق العمل في مجال الأمن السيبراني واعد جدا والطريق امام المتخصص مليئ بالفرص الوظيفية التي تهدف الى تعزيز الأمن السيبراني للدولة

وحماية مصالحها الحيوية وأمنها الوطني والبنى التحتية الحساسة ومن هذه التخصصات ما يلي :-

1. هندسة الأمن السيبراني
2. الأمن السيبراني الألي
3. حوكمة الأمن السيبراني وإدارة المخاطر
4. عمليات الأمن السيبراني الدفاعية.
5. إدارة برنامج الأمن السيبراني.
6. مخاطر تهديد الأمن السيبراني
7. قيادة الأمن السيبراني التنفيذية
8. اختبارات الاختراق والأختراق الأخلاقي
9. الاستجابة للحوادث

لقد أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعيشه في العالم وحاجة اردنية ملحة لما له من أهمية في أمن المعلومات، حيث يشهد العالم المتقدم بكافة أرجائه تطور كبير جعل مقصد الكثيرين من الدارسين المتميزين حول العالم يركزوا على الدراسات التكنولوجية في مجال الحوسبة الرقمية . (الدستور 2022)

تحديات الأمن السيبراني في الأردن:

هناك عدة تحديات تواجه الأمن السيبراني في الأردن تتمثل فيما يلي: (جريدة الغد الأردنية، 2022)

إنترنت الأشياء:

ذكرت الاستراتيجية الوطنية للأمن السيبراني في الأردن بأن اول التحديات يتمثل في توجه تقني حديث هو " إنترنت الأشياء" حيث ان هذه التقنية تزيد من عدد الأجهزة المتصلة بالإنترنت لزيادة فرص النمو الاقتصادي والادماج والحراك المجتمعي والتواصل وابتعاد فرص عمل جديدة وما تزال المنهجيات الهادفة الى تحقيق امن " إنترنت الأشياء" تعاني ثغرات في أحيان، وهو ما يتيح المجال امام المجرمين السيبرانيين لاستغلالها في شن هجمات الكترونية.

واضافت الاستراتيجية بأن اعتماد الحكومات والشركات على إنترنت الأشياء الصناعية يزيد بحيث يمكن للأجهزة استغلال تكنولوجيا الاتصالات لمراقبة وجمع وتبادل وتحليل كميات ضخمة من البيانات من اجل توجيه عملية صنع القرار بشكل اسرع وافضل وهو ما يستدعي الاحتياط وتوفير القدرات لمجابهة اي اختراقات لهذه الأنظمة.

برمجيات الفدية:

وأكدت الاستراتيجية الوطنية للأمن السيبراني الأردني بأن شهرة البرمجيات الخبيثة نمت كإحدى ادوات الهجوم القادرة على تشفير او تدمير الملفات بشكل مطرد بعد ان ثبت نجاحها ومن المتوقع ان يكون استخدامها احد اهم اشكال الهجمات السيبرانية في المستقبل.

الذكاء الاصطناعي:

فيما أضافت الاستراتيجية الوطنية بأن تقنية الذكاء الاصطناعي تعد اليوم من التحديات الكبيرة في مجال الأمن السيبراني حيث ان المجرمين يستخدمون الذكاء الاصطناعي في نشر اعلانات وارسال رسائل بريد الكتروني متصيدة اكثر استقطابا

لفئات محددة في الفضاء السبراني وذلك من خلال تحليل كم كبير من المعلومات المتأتية من وسائل التواصل الاجتماعي لتحديد الفئات المستهدفة، كما من الملاحظ كذلك تزايد استخدام نظام الدردشة على الإنترنت لغايات خدمة الزبائن وهو ما يكسب هذا النظام ثقة الجمهور وعليه سيسعى المهاجمون الى استغلال هذه الثقة وانشاء منصات دردشة للحصول على بيانات مالية من الناس.

التطبيقات التي لا تعتمد على الخوادم:

وتفيد الاستراتيجية الوطنية للأمن السبراني بأن المعلومات تواجه خطرا كبيرا نتيجة استخدام تطبيقات لا تعتمد على الخوادم على الأجهزة الشخصية، فعند التخزين على الخوادم يكون مالك المعلومات اكثر قدرة على اختيار الاحتياطات الأمنية الضرورية لضمان الحفاظ على خصوصية بيانات المستخدم لحماية البيانات من سارقي الهوية وغيرهم من المجرمين السبرانيين، اما مع استخدام التطبيقات التي لا تعتمد على خوادم فتكون تلك الاحتياطات من مسؤولية المستخدم الى حد كبير.

البنية التحتية الحساسة:

وتتضمن الاستراتيجية الوطنية بأن مؤسسات البنية التحتية الحساسة كندي للأمن السبراني في الأردن تعتمد بشكل كبير على أنظمة التحكم الصناعية المتصلة مع بعضها بعضا لإدارة مختلف جوانب اعمالها الأمر الذي يزيد من فرص المهاجمين لاعتراض تلك الأنظمة والأجهزة بهدف الحصول على مكاسب اقتصادية او سياسية.

حملات التصيد المتطورة:

وتضيف الاستراتيجية الوطنية للأمن السبراني بأن هناك تزايدا وتطور في رسائل التصيد الإلكترونية التي تستخدم عادة لنشر برامج خبيثة او لتحفيز الضحايا للافصاح

عن بياناتهم الشخصية خاصة بعد اضافة معلومات معينة عن الشركة مثل معلومات الفواتير والشؤون اللوجستية وغيرها.

الاستخدام الاستراتيجي لعمليات المعلومات:

حيث تفيد الاستراتيجية الوطنية للأمن السيبراني بأن الهجمات وعمليات التجسس السيبرانية ونشر المعلومات المغلوطة (الاخبار الزائفة) تعتبر من الأدوات المستخدمة بشكل متزايد من قبل عدد من الدول والافراد لخلق الاضطرابات السياسية والاقتصادية.

الحوسبة السحابية:

أكدت الاستراتيجية الوطنية للأمن السيبراني بأن تقنية الحوسبة السحابية وتوسعها وانتشارها بما تشتمل عليه من بيانات كثيرة اليوم تعد تحديا في مجال الأمن السيبراني، حيث يزداد استخدام المؤسسات للتقنيات السحابية التي تسمح بالاستجابة لاحتياجات الأعمال المتزايدة بشكل اكثر سرعة ومرونة ويكمن التحدي الرئيس هنا في ادارة مخاوف الأمن والخصوصية من قبل مقدمي الخدمات السحابية.

الوعي بالأمن السيبراني:

وأشارت الاستراتيجية الوطنية للأمن السيبراني إلى تحدي الوعي، وقالت بانه لا يزال الوعي العام بالأمن السيبراني محدودا نوعا ما، ما يضعف بشكل كبير الجهود المبذولة لحماية المعلومات الحساسة.

خدمات القرصنة مقابل أجر:

وتعزي الاستراتيجية الوطنية بانه بسبب توافر الأدوات وسهولة استخدامها وانخفاض تكاليفها اصبح بإمكان مجموعات القرصنة تقديم خدمات القرصنة مقابل اجر بشكل اسهل من اي وقت مضى وهو ما يشكل تحديا جديدا في الفضاء السيبراني.

نقص المهارات:

وأكدت الاستراتيجية الوطنية للأمن السيبراني على ان نقص مهارات المهنيين المعنيين بشؤون الأمن السيبراني يعتبر مشكلة عالمية ما تزال مقلقة للقطاعين العام والخاص، وتسعى الى تحفيز الاشخاص والخريجين في مجالات الحاسب والهندسة الحاسوبية الى الانخراط في مجالات متعددة لاكتساب خبرات ومهارات في مجالات الأمن السيبراني.

المبحث الثالث: ادارة الخطر السيبراني

على مدى السنوات الثلاثين الماضية، ازداد اعتماد الحكومات والشركات والمواطنين على الإنترنت وعلى تقنيات المعلومات والاتصالات " ICTs " بشكل كبير ونفترض أن الخدمات الاساسية المقدمة للمواطنين مثل الكهرباء والاتصالات ستبقى تعمل على الدوام وأن البضائع والخدمات والبيانات ورؤوس الاموال ستعبر الحدود بكل سلاسة، ولكن العديد من الأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر وتعرض للاستغلال حيث تواجه شتى أنواع المؤسسات خروقات للبيانات بانعدام الأمن آخذ بالنمو.

وتمتّع أكثر من 100 وتعرض الأنشطة إجرامية وتتعلّل خدماتها وتُدمر ممتلكاتها. وإحساسنا جميعاً دولة بالاضافة إلى عدد متزايد بسرعة من الجهات غير الحكومية والافراد بالقدرة على إيذاء البنى التحتية المتصلة بالشبكات التابعة للحكومات ولقطاعات الصناعة.

وتختلف أهداف هذه الجهات من جهة أخرى وتتراوح من النشاط السياسي إلى الاحتيال والجريمة الإلكترونية وسرقة الممتلكات الفكرية ، والتجسس وتعطيل الخدمات وتدمير الممتلكات والاصوةل، وتعيش الدول والشركات في عالم يسوده انعدام الأمن السيبراني - فجميع الحكومات والشركات التجارية والافراد يواجهون مخاطر سيبرانية ويتشاطرون مستوى من المسؤولية في إدارة هذه المخاطر. وكما أكّدت الاحداث الاخيرة في عدة دول ينبغي على الدول والشركات أن تدرك أولاً الأخذ بإجراءات مفادها أن استراتيجيتها وأجندتها الرقمية ينبغي أن تكون قائمة على منهج منضبط ادارة المخاطر. فالتراخي وعدم اتخاذ الإجراءات المناسبة له مخاطر جمه.

أطر العمل لفهم الخطر السيبراني:

تعمل الدول والمنظمات الدولية والمؤسسات الأكاديمية على تطوير أطر عمل لمساعدة قادة الحكومات والشركات على تشخيص الخطر السيبراني وعلى خفضه، وهناك حاجة كبيرة لأطر العمل هذه الآفة على مدى العقود الثلاثة الماضية اقتنع نفس هؤلاء القادة بمزايا و"فوائد" تقنيات المعلومات التجارية، بما فيها زيادة الانتاجية، وزيادة الفعالية، وانخفاض تكاليف المعدات الرأسمالية وتخزين البيانات ومعالجتها والنمو الصافي ولكنهم اجلوا الاستثمار في أمن ومرونة بناهم التحتية المتصلة بالشبكات ومؤسساتهم التجارية الرقمية، وان النشاطات السيبرانية المدمرة والمعطلة في يومنا هذا تُحتم على هؤلاء القادة مواجهة انعدام الأمن الذي زرعه من دون قصد في صلب المجتمع، فالخسائر آخذة بالتراكم، والاذى آخذ بالنمو، والخطر مُحقق. (المعهد الوطني للمعايير والتقنية، 2017)

أطر العمل الحكومية:

لقد بدأت الحكومات بتطوير أطر عمل وعلامات استدلالية واستراتيجيات وطنية واسعة لفهم مواضع اعتمادها على البنية التحتية للإنترنت ومواضع الضعف بشكل أفضل ومن أجل تأمين الشبكات والبنى التحتية والخدمات الوطنية التي يعتمد عليها مستقبلها الرقمي ورفاهها الاقتصادي، وعندما يتعلق الأمر بالتخطيط وجذب الانتباه للخطر السيبراني لدولة ما يكون السؤال الملح: كيف يمكن تشخيص وتقليل خطر تراكم على مدى 30 سنة؟

إن من المهم البدء بفهم الخطة الاستراتيجية للدولة والتي تستغرق من 3-5 سنوات وتحديد الأمور التي يمكن القيام بها لتحقيق ذلك الهدف على المدى البعيد،

وعلى سبيل المثال، تشير تقديرات الهولنديين إلى أنه بحلول عام 2020، سيشكل الاقتصاد الرقمي أي البضائع الرقمية والخدمات الإلكترونية، ما لا يقل عن 25% من إجمالي الناتج المحلي للدولة، وأكدت هولندا أن مستقبلها يعتمد على قدرتها على تأمين اقتصادها الرقمي، وهي تقوم ببعض الاستثمارات والصلاحيات الهيكلية الضرورية للتمكن من تحقيق ذلك الهدف، وتعمل بلدان أخرى، مثل الولايات المتحدة وألمانيا، على تحديد الشركات الكبرى التي تشكّل أكثر من 2% من إجمالي الناتج المحلي للدولة وتعمل معها لتكون إدارة المخاطر والمرونة جزءاً من عملياتها الشاملة لتخطيط الأعمال.

إلا أن معظم الدول الأخرى قد اتخذت نهجاً أوسع وطالبت بحماية "البنى التحتية الحساسة"، أي ما يتعلق بالأصول والأنظمة والشبكات الأساسية التي يُعتقد بأنها أصبحت مع مرور الوقت غير حصينة للخطر دون غيرها من الشبكات من خلال ازدياد الترابط والاعتماد على الإنترنت، وبالتالي، تكون عرضة لفشل المعدات والخطأ البشري والأحوال الجوية والقطاعات الأخرى الناجمة عن العوامل الطبيعية، والهجمات المادية والسيبرانية.

التحدي الذي يواجه هذا النهج:

إن التحدي الذي يواجه هذا النهج هو عدم تحديد المسؤولية بشكل واضح بين الحكومة والقطاع مما يُصعب من تحميل المسؤولية لأي شخص بسبب تقاعسه، لعدم وجود التزام بخفض الخطر وبزيادة المرونة، وفي هذه الأثناء، انعدام الأمن آخذ بالنمو في المجتمع ونظراً لهذا قررت بعض الحكومات أن الوقت قد حان للتدخل في

السوق، وهي تستخدم أنظمة وقوانين الالزام لبعض القطاعات بتحديد وتقييم وتصحيح مواضع القصور في وضعها الأمني.

وتشمل القطاعات الخاضعة للتنظيم: مرافق الكهرباء، الخدمات المالية، الرعاية الصحية، النقل والإتصالات، ومن بين الاجراءات التنظيمية الاخرى التي تتبناها الدول إلزام السلطات المحلية أو الوطنية بإرسال الاشعارات والتبليغ عن أي خرق يحدث مع ذكر نوع البيانات التي تعرضت للخطر أو التي فُقدت والتقنية ، أو الوسيلة المستخدمة في الخرق، ومعلومات عن أي انقطاع أو تعطل للاعمال التي تتعلق بالإتصالات في حال وقوعه، ويفرض الاتحاد الاوروي هذه الانواع من المناهج الالزامية على بناء التحتية الحساسة وعلى مشغلي الخدمات الاساسية، وتبنى الاتحاد الاوروي نظاما لتوجيه الاتحاد حول أمن الشبكات والمعلومات .

التمتع بالجاهزية السيبرانية:

بالرغم من توفر العديد من النماذج وأطر العمل في وقتنا هذا لقادة الدول ليقوموا بتشخيص وخفض الخطر السيبراني في بلادهم، وبالرغم من الدعوات العديدة من أخصائيي هذا المجال ومن خبراء الأمن السيبراني اتخاذ الاجراءات المناسبة للتحسين على مستوى الأمن السيبراني على المستوى الوطني لا يزال يشكل تحديا حيث اعترفت هولندا بأن صحة الاقتصاد في المستقبل تعتمد على الاقتصاد الرقمي الموثوق، وحسن الاداء وبالتالي خصصت الاموال المناسبة وقامت بتأسيس مركز لضمان تحقيق الدولة لاهدافها بشكل آمن.

وقد تم إجراء "مراجعة لسياسة البنى التحتية الحساسة"، وفي تلك المراجعة، عرفت الحكومة البنى التحتية الحساسة بأنها "مجموعة من المنتجات والخدمات

والعمليات التابعة لضرورة لعمل الدولة، وأنها ينبغي أن تكون آمنة وأن تتمكن من الصمود ومن التعافي بسرعة من جميع التحديات والهجمات ولكن عندما تأثر ميناء روتردام أكبر ميناء في أوروبا بشكل كبير وانشلت خدماته بفعل "Not Petya" في 2017 وبدأ المسؤولون بفحص وضعية الميناء من حيث مواضع اعتماده على الإنترنت، واكتشفوا أن البنية التحتية للميناء لم تكن تُعتبر من بين البنى التحتية الحساسة في استراتيجيتهم الوطنية للأمن السيبراني وفي سياساتهم لحماية البنى التحتية، وفي الوقت نفسه، حتى المملكة المتحدة التي حددت قطاعات حساسة معينة مثل قطاع الرعاية الصحية، الذي ينبغي أن يتماشى مع معيار محدد للرعاية، ولم تعتقد بأن مزودي خدمات الرعاية الصحية فيها مستعدين للاستثمار لتحديث برمجياتهم ولحماية خدمات المرضى الحساسة من المخاطر السيبرانية وبالتالي، عندما وقعت أكثر من 81 منظمة من منظمات هيئة الخدمات الصحية الوطنية البالغ عددها 236 منظمة ضحية لبرنامج الفدية البسيط " Wanna Cry " أدت هذه الحادثة البسيطة التي كان جُبرت المملكة المتحدة على التأكد فيما إن كان بالإمكان تفاديها بكل بساطة تعريض حياة الناس للخطر.

تقييم الخطر:

ينبغي على قادة الدول ذكر نيتهم بوضوح للاستفادة من البيئة الرقمية لتحقيق الازدهار الاقتصادي والاجتماعي من خلال خفض المستوى العام لخطر الأمن الرقمي داخل الحدود وعبرها، وينبغي أن يدركوا أن الخطر يتغير مع مرور الوقت بالاعتماد على الاجراءات التي يتخذها طرفان على الاقل هما: المهاجم الذي يحصل على القدرة لاحداث الضرر ويستخدمها، والطرف المستهدف الذي يمكنه

أخذ الاحتياطات لتحمل أو لاحباط الخطر الذي يتسبب به المهاجم، وينبغي على قادة الدول ابداء التزامهم بخفض المخاطر ويزيادة المرونة من خلال إجراء تقييمات مستمرة للخطر على الصعيدين الوطني والقطاعي وتبني الاجراءات والسياسات والعمليات المناسبة لادارة المخاطر التي يتم تحديدها، ومن أجل تحقيق هذه الأهداف الشاملة ينبغي على قادة الدول ،وعلى صانعي السياسات وأصحاب المصلحة المعنيين الاخرين في لتقييم الخطر. (مجلس منظمة التعاون الاقتصادي والتنمية، 2015)

هل توجد خطوط واضحة للمسائلة والمسؤولية لضمان تنفيذ أهداف الدولة وتطبيق إجراءات خفض المخاطر؟ أساسياً من عملية التخطيط؟، هل كانت اعتبارات الأمن السيبراني والمرونة جزءاً هذا التقييم الشامل والمتكامل سيرز مواضع الاعتماد الرقمي الكثير حساسية في الدولة، أي الشركات والخدمات والبنى التحتية والأصول التي إن تعرضت للأذى، سيكون لذلك عواقب وخيمة على إقتصاد وأمن الدولة، لن يتمكن صناع القرار من اتخاذ الاجراءات التصحيحية الإحباط أو خفض المخاطر، الا بعد تحديد الأمور غير الحصينة، وما قد يُهدد أمن أصول الدولة، واحتمالية تعرضها للخطر، أو الذي أو الضياع.

خفض المخاطر من خلال التخطيط الدقيق:

بعد الانتهاء من إجراء تقييم المخاطر، يمكن للدولة وضع خطة لخفض المخاطر لسد الفجوة بين وضعيتها الحالية من ناحية الأمن السيبراني وبين القدرات السيبرانية الوطنية اللازمة لتصحيح مواضع القصور ولدعم مستقبل الدولة الاقتصادي وأولوياتها الأمنية، وينبغي أن تكون جهود خفض المخاطر بقيادة سلطة وطنية كفوءة

ومختصة في مجال الأمن السيبراني، أي قائد "شخص أو مؤسسة على حد سواء" ذو مكانة عالية وراسخة في أعلى درجات الحكومة لتقديم التوجيهات ولتنسيق الاجراءات للمسائلة بالنسبة لمواضع القصور وللتناج المتحققة، بما أن الأمن السيبراني يتقاطع ومراقبة تنفيذ الخطة بحيث يكون خاضعاً مع العديد من المجالات الأخرى مثل حقوق الإنسان، والتنمية الاقتصادية، والتجارة، وضبط الأسلحة والاستعمال المزدوج للتقنيات، والأمن، والاستقرار، والسلم وحل النزاعات، من الهام ضمان تمتع السلطة الوطنية المختصة بالسلطة الموضوعية وبالمسائلة وبالتمكين لضم وتوجيه العدد الالزم من أصحاب المصلحة، بالرغم من كثرة التوجيهات المتعلقة بنشاطات خفض المخاطر كما يتضح من أطر العمل المتنوعة الموضحة في الاقسام السابقة، إلى أنه ينبغي على قادة الدول بذل جهود أكبر لفهم طبيعة الخطر السيبراني، والتهديدات المحددة التي تواجه البنى التحتية المتصلة بالشبكات، والتي ينبغي أن توصف بدقة ووضوح في استراتيجياتهم للأمن السيبراني الوطني وفي تقييم، او اجراء تقييمات الخطر السيبراني الوطني، ومن ثم العمل مع جميع أصحاب المصلحة المعنيين لتخطيط دفاعاتهم بشكل أفضل، ولتعيين الموارد البشرية والمالية لخفض تلك المخاطر، وتشمل الاستراتيجيات الشائعة لخفض المخاطر السيبرانية بشكل فعال: (مجلس منظمة التعاون الاقتصادي والتنمية، 2015)

أ. تحديد الأمور المعرضة للخطر وزيادة الوعي العام بالمخاطر في جميع المستويات من قادة الحكومات إلى المواطن العادي، لا يمكن للناس إعطاء الأهمية للأمن من دون أن يفهموا أولاً مدى تعرض نشاطاتهم اليومية، وليس مجرد معلوماتهم الشخصية للخطر، بالتالي، ينبغي أن تبادر الحكومة بإنشاء حملة

وطنية لزيادة الوعي العام، وتعزيز التعليم والتدريب، وتنمية المهارات وتمكين مواطنيها ليصبحوا جزءاً من الحل ببناء ثقافة قوية للأمن السيبراني.

ب. تحديد الموارد الالزامية وترتيبها حسب الأولويات المطلوبة وتركيزها على الأصول عالية القيمة وعلى الأنظمة ذات الأثر العالي التي تتطلب مستويات إضافية من الحماية وعلى الجهات الأكثر حساسية في الدولة المعتمدة على التقنية الرقمية، مثل الشركات والبنى التحتية والخدمات والأصول، وفهم نقاط ضعفها، وإعطاء الأولوية للإجراءات الأمنية المناسبة والمتناسبة مع الخطر الاقتصادي المجتمعي.

ت. إعداد أطر عمل قانونية وتنظيمية مناسبة لحماية المجتمع من الجريمة السيبرانية ومن انقطاع الخدمات وتدمير الممتلكات.

الفصل السادس

السببرانية ساحة الحرب القادمة

المبحث الأول: ما هبة ساحة الحرب القادمة

إنَّ العالمَ يَعيش منذ نهاية القرن العشرين ثورة في مجال المعلوماتية وبصورة خاصة في نطاق تكنولوجيا المعلومات ووسائل الاتصال. وكانت شبكة الاتصال بين أجهزة الكمبيوتر، أو الحاسب الآلي أو الحاسوب قد نشأت في بداية الأمر في العام 1969 لخدمة الأغراض العسكرية للولايات المتحدة الأمريكية الأربنت "Arpanet"، التي اتخذت القرار بإطلاقها على مستوى العالم لخدمة أهداف المعرفة والتواصل بين مختلف المجتمعات، الإنترنت فقامت بعض الشركات المتخصصة بإنشاء نظام يَسمح بتيسير الاتصال والتواصل والتعارف بين البشر "بروتوكالات الاتصال"، مثلاً، وأنشأت كيانات تُتيح لكل شخص أو شركة الحصول على صندوق بريد إلكتروني "Email"، وعلى مواقع على الشبكة العنكبوتية العالمية "World Wide wip" التي يُمكن الدخول إليها والاطلاع على المعلومات المتوافرة من خلالها، وإنَّ "العديد من وسائل السيطرة والتحكم الخاصة بمُعظم العمليات الحيوية الموجودة على الأرض انتقلت إلى الفضاء في صورة أقمار صناعية ومحطات فضائية، كما انتقل أيضاً قطاع واسع من الحروب والمعارك والحوارات والثورات إلى العالم الافتراضي الذي صنعه الإنسان منذ اختراعه الكمبيوتر والذاكرات الإلكترونية وشبكات المعلومات، فأنشأ داخله جغرافية افتراضية جديدة. (عكاشه، 2012)

إنَّ هذا التطور أتاح التعامل الدولي بأسلوب جديد لم يَكُن ملحوظاً أو مُتوقَّعاً عند وَضْع النُّظْم القانونيَّة السائدة. فبعد أن كان التعامل الدولي خلال المنازعات المُسلَّحة يتمُّ على الأرض أو البحر أو الجو أو الفضاء الخارجي، أصبح، بفعل هذه التقنيَّة، يتمُّ بطريقة إلكترونيَّة ضمن نظام معلوماتي يَخْتلف كلياً عن الحرب البريَّة والبحريَّة والجويَّة، إنَّ لجهة اختراق منظومة العدو الإلكترونيَّة أو لجهة جمع المعلومات الإلكترونيَّة الحسَّاسة أو نقلها أو تبادلها.

ومع تزايد الاعتماد على الوسائل التقنيَّة الحديثة في إدارة الأعمال المُختلفة، برَزَت تحدِّيات قانونيَّة وطُرحت تساؤلات حول إمكان اعتبار التواصل الإلكتروني الافتراضي "Virtual communication" الذي أصبح يتم اليوم بواسطة الإنترنت، أو الفضاء الإلكتروني أو الفضاء السيبراني "Cyberspace"، مُوازياً للمرافق العامَّة الدوليَّة التقليديَّة، وحول ضرورة عقد معاهدات جديدة تتَّسجِم مع التطوُّر التكنولوجي إنَّ لم تكن الإمكانية الأولى مُتاحة أو كافية.

إنَّ الفضاء السيبراني غداً إذاً مُنافساً حقيقياً للنطاق الدولي التقليدي، من بحر وجو وفضاء خارجي، وقد يأتي يوم ينكفي فيه استعمال هذا الأخير لمصلحة الأول. على الرغم من ذلك، يبقى أنَّ ثمة مرحلة انتقاليَّة لا بُدَّ من المرور بها وصولاً إلى بلورة الوضع القانوني الخاص بالفضاء السيبراني. ومن معالم هذه المرحلة أنَّ الثقافة القانونيَّة التي لاتزال إلى حدٍّ بعيد مُشبعة بمفهوم النطاق الدولي التقليدي، أو الواقعي أو الحقيقي تميل إلى جَعْل وضع هذا الأخير القانوني مقياساً لنجاح الفضاء السيبراني. بمعنى آخر، كلُّما تمَّ التَّصديق على معاهدات أو ترسَّخت مواقف اجتهادية أو ظهرت آراء فقهيَّة تذهب إلى إعطاء الفضاء السيبراني وضعاً قانونياً، فإنَّها تتَّخذ من النطاق

الدولي التقليدي مثلاً تَحْتَذِيهِ لجعل الفضاء السيبراني قابلاً للانضمام إلى النُظُم القانونية السائدة أو المعروفة. تعرضت ظاهرة الصراع إلى تغييرات مع بروز الفضاء الإلكتروني، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات. وهنا، برز “الصراع السيبراني” كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولاً أم غير دول في الفضاء الإلكتروني.

وبرغم الآثار المدمرة لهذا النمط من الصراعات، فلا يرافقه دماء، وقد يتضمن التجسس والتسلل إلى مواقع الخصوم الإلكترونية، وقرصنتها، دون أنقاض، أو غبار. كما أن أطرافه يتسمون بعدم الوضوح، وتنطوي كذلك تداعياته على مخاطر عدة على أمن الدول، سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعددة.

ومع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه، اتسعت دائرة الصراعات السيبرانية، وزاد عدد المهاجمين، وباتت هناك حالة من الكر والفر في الهجمات الإلكترونية لتعبر عن الصراع الممتد، ولذا، صار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة، والتفوق، والهيمنة، وتعزيز التنافس حول السيطرة، والابتكار، والتحكم في المعلومات وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي. (Myriam, 2001)

وبما أن المتنازعين يلجئون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة، فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني، وكان لهذا التغيير دور في إعادة التفكير في حركية وديناميكية الصراع، بل وبروز ما يعرف "بعصر القوة النسبية". وعنت هذه الأخيرة أن القوة العسكرية قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلق آثارا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي.

وأسهم عاملان رئيسيان في انتشار رقعة الصراع في الفضاء الإلكتروني، وبالتالي إفساح المجال لنشوء الحروب السيبرانية، وهما:

أ. تغير منظور الحرب جذريا، حيث انتقلت من نسق "الحروب بين الدول إلى وسط الشعوب" فكان الغرض من الحرب قديما هو تدمير الخصم، إما باحتلال أرضه، أو الاستيلاء على موارده. أما الحروب الجديدة، فقد استهدفت بالأساس التحكم في إرادة وخيارات المجتمعات. ومن ثم، بدا للشعوب أهمية محورية في هذا النمط الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

مع هذا التغير، أصبحت أهداف الحرب أقل مادية، وتركزت أكثر على العامل النفسي والدعائي، لاسيما مع تنامي التغطية الإخبارية، والسمعية، والبصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات، وضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

ب. بروز الصراعات ذات الأبعاد المحلية - الدولية، حيث ساعد اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك طبيعة السياق الدولي للفضاء الإلكتروني، في توفير بيئة مناسبة لدمج الفئات والقوي المهمشة في السياسة الدولية، وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية، أو انتماءات عرقية أو دينية.

إذ أسهم الفضاء الإلكتروني في دعم الهياكل التنظيمية والاتصالية للحركات والجماعات المحلية، والمنظمات المدنية، بما ساعد الفاعلين من غير الدول على ممارسة قوة التجنيد، والحشد، والتعبئة، واستجلاب التمويل.

وهنا، تختلف أهداف الحروب الإلكترونية وفقا لطبيعة أهداف الصراعات السيرانية، وذلك على النحو الآتي:

1. صراع سيراني ذو طبيعة سياسية، حيث تحركه دوافع سياسية، وقد يأخذ شكلا عسكريا يتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية. ويتضمن هذا النوع من الصراعات توظيف أسلحة إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون مع قوي أخرى لتحقيق أهداف سياسية (. عادل، 2007)

2. صراع سيراني ذو طبيعة ناعمة، أي الصراع حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية. ويتم ذلك من خلال تسريب المعلومات، واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية.

3. صراع سيبراني على التقدم التكنولوجي، حيث يأخذ هذا النمط من الصراعات السيبرانية طابعا تنافسيا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية. وقد يمتد إلى محاولة للسيطرة على الإنترنت، وأسماء النطاقات، وعناوين المواقع، والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول، بدون استخدام طائرات، أو متفجرات، أو حتي انتهاك حدود الدول، كهجمات قرصنة الكمبيوتر، وتدمير المواقع والتجسس، بما قد يكون له من تأثيرات مدمرة في الاقتصاد، والبنية التحتية بذات قوة التفجير التقليدي.

4. صراع سيبراني على المعلومات والاستخبارات. فمع صعوبة الفصل بين أنشطة الاستخبارات، وجمع المعلومات، وحروب الفضاء الإلكتروني، أو التمييز بين الاستخدام السياسي والإجرامي، يبدو الفضاء الإلكتروني بيئة أكثر مناسبة للصراعات المعلوماتية. إذ يسهم في دعم قدرة الأجهزة الأمنية للدول، أو حتي الجماعات المختلفة، على تشكيل شبكة عالمية من العملاء بدون تورط مباشر، بالإضافة إلى رخص التكلفة، وسهولة الاتصال، وصعوبة الرقابة التقليدية على التفاعلات الإلكترونية، ومثل ذلك عنصرا جذبا لاستخدام الأسلحة الإلكترونية، وتوظيفها لتحقيق أهداف سياسية وعسكرية.

ويمكن طرح عدة أنماط لهذه الحروب من حيث مدي درجة شدة الصراع من عدمه، ومن أبرزها:

النمط الأول: الحرب السيبرانية الباردة منخفضة الشدة: حيث يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة. ويعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي

أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة ثقافية، أو اقتصادية، أو اجتماعية. وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شن حرب إلكترونية واسعة النطاق.

ولهذه الحرب السيبرانية الباردة وسائل عدة، منها شن الحروب النفسية، والاختراقات المتعددة، والتجسس وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية. وتجلي هذا النمط في حالات الحروب في الصراعات السياسية، ذات البعد الاجتماعي - الديني الممتد، مثل الصراع العربي - الإسرائيلي، أو الصراع الهندي - الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية، وغيرها. (David, 2012)

في مثل هذه الصراعات، تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية، مثل جماعة "ويكيليكس"، و"أنونيموس"، وكذلك أيضا في حالات الأزمات الدولية، مثل التوتر بين استونيا وروسيا في عام 2007، وكذا الاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين طهران وواشنطن.

وقد تعرضت روسيا للاتهام بالقرصنة الإلكترونية في الانتخابات الأمريكية الأخيرة لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلينتون، كما تم اتهام روسيا بشن هجمات إلكترونية على النرويج، والتشيك، وبريطانيا، مما دفع الدول الأخيرة لإعلان أنها قادرة على الرد بالمثل.

وشنت إيران هجمات إلكترونية على منشآت نفطية في منطقة الخليج العربي، احتجاجاً على مزاعم بتعرض الأقليات الشيعية للتمييز، كما الحال مع هجمات فيروس "دوكو" في عام 2012، وهجمات فيروس "شمعون 2" ضد السعودية في يناير 2017. (Britain, 2017)

النمط الثاني: غطت الحرب السيبرانية متوسطة الشدة: حيث يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة على الأرض. ويكون ذلك تعبيرا عن حدة الصراع القائم بين الأطراف، كما قد يهدف لعمل عسكري. هنا، تدور حروب الفضاء الإلكتروني عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشن حرب نفسية ضد الخصوم، وغيرها.

ويستمد ذلك النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تشكل أربعة أضعاف من إنفاق نظيراتها التقليدية، مما يمكن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابه.

وتاريخياً، تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم. أيضاً، برزت خلال الحرب بين حزب الله وإسرائيل في عام 2006، وكذلك بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في عامي 2008 و2012.

النمط الثالث: الحرب السيبرانية "الساخنة" مرتفعة الشدة: حيث يعبر ذلك النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية

التقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد بين الدول والفواعل من غير الدول على الفضاء الإلكتروني.

ينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية.

وفي هذا السياق، يتم أيضا استخدام الفضاء الإلكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة أولي لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتي باستهداف الحياة المدنية، والبنية التحتية المعلوماتية. والهدف من وراء ذلك تحقيق الهيمنة الإلكترونية الواسعة بشكل أسرع في حالة نشوب صراع.

وقد شهدت الأسلحة الإلكترونية تطورا أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة، والهجمات الإلكترونية عبر الفيروسات، مثل شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010، وكان قد تم تطوير هذا الفيروس وتجربته في إسرائيل خلال عام 2007. (Robert, 2010)

المخاطر والتداعيات:

أدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1. تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت. وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب. (عادل، 2016)

2. تعزيز القوة وانتشارها، فمن جهة، عزز الفضاء الإلكتروني ما يسمى بـ “القوة المؤسسية” في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية (josep,2011).

من جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولاً، أم من غير الدول.

3. عسكرة الفضاء الإلكتروني، وذلك سعياً لردء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع

والأمن الإلكتروني، وتساعد القدرات في سباق التسلح السيرياني، وتبني سياسات دفاعية سيريانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيريانية داخل الجيوش الحديثة.

4. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم. وهنا، ترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة. (Nakashima, 2012)

6. تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيريانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا، يتعلق

التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى. (شكري، 2019)

لكن تبقى مشكلة دخول العالم سباق التسلح السيبراني " A Cyber Arms Race " في تحديد ماهية تلك الأسلحة التي يمتلكها الآخرون، حيث لا يملك المجتمع الدولي قدرة سريعة على التدخل لاحتوائها، ولا يوجد مجال لتفعيل التفتيش كآلية مراقبة، مثل حالة الأسلحة النووية.

وإن كانت عملية بناء القدرات العسكرية في مجال الأسلحة الإلكترونية تنطوي على عناصر أساسية، منها أولا السعي إلى امتلاك التكنولوجيا، وأنظمة الحماية، وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني، وثانيا تطوير القدرات الهجومية، إما عبر بناء القدرات الذاتية، أو بالاستعانة بالأفراد والشركات المتخصصة، وتطوير القدرة على اختبار مدي الجاهزية لمواجهة الهجمات الإلكترونية، وثالثا وأخيرا، العمل على توفير الميزانيات المخصصة لتطوير القدرات الهجومية والدفاعية، وخاصة مع قلة تكلفتها، مقارنة بحجم ما ينفق على الجيوش التقليدية.

المبحث الثاني: مستقبل الحروب السيبرانية

ذكر تقرير أعده مار بوميلو في إصدار خاص في دورية "Cyber Defense Review"، وهي دورية يصدرها معهد الجيش السيبراني الأمريكي في ويست بوينت، أن الجنرال فوغارتي، قائد القيادة الإلكترونية للجيش الأمريكي "ARCYBER"، قدم خارطة طريق مكونة من ثلاث مراحل يتم تنفيذها من قبل القيادة السيبرانية للجيش الأمريكي على مدى عشر سنوات، والتي انتهت المرحلة الأولى منها في منتصف العام 2021، والتي تهدف إلى تحديد ملامح الأسس التي ستقوم عليها الأهداف الأمريكية المتعمقة بالتحضير للأخطار الجديدة في الحرب السيبرانية وهي الآتية : (<https://www.aljundi.ae>)

المرحلة الأولى:

تحقيق الإنشاءات الأولية للبرامج والتشكيلات الجديدة، والتي تم تنفيذ العديد منها لبعض الوقت. حيث يتمثل الجهد الرئيسي في نقل مقر القيادة من فورت في ولاية فيرجينيا، إلى فورت في ولاية جورجيا، والذي يهدف إلى تمكين القوات السيبرانية العملياتية والمؤسسية في الجيش الأمريكي من العمل بتآزر غير مسبوق من خلال منصة عرض طاقة معلوماتية واحدة.

وتعد كتيبة دعم الحرب الإلكترونية "915" أحد الكيانات الجديدة نسبياً حيث تتكوف الكتيبة، التي تم إنشاؤها في العام 2019، والمكونة من 12 فريقاً تدعم فرق الأولوية القتالية أو غيرها من التشكيلات التكتيكية. وتساعد فرق التحقيق في أفاق بعيدة، كما يسميها بعض المسؤولين، في التخطيط للعمليات الإلكترونية التكتيكية للقادة في مسرح العمليات وتنفيذ المهام في جانب واحد بالتنسيق مع القوات في ميدان القتال.

وقد لاحظ المسؤولون سابقاً ان هذا التشكيل من المرجح ان يتم تطويره على مر السنين: بينما تجري القوة عمليات وتدريبات، فرمما تحتاج إلى إعادة النظر في هيكلها وقدراتها، كما ستخضع القيادة، بحسب فوغارتي لعملية إعادة تنظيم لزيادة عدد فرق دعم عمليات المعلومات الميدانية المتاحة، وتوسيع نطاق الوصول إلى الخلف وقدرات وسائل التواصل الاجتماعي لتشمل كل من قوات العمليات التقليدية والخاصة.

المرحلة الثانية: ووفقاً لخارطة الطريق، فإن المرحلة، التي ستتم ما بين العام 2021 و2027، هي المكان الذي سيتم تجريب القوة فيه وتبتكر، حيث ستشهد هذه المرحلة توظيف القدرات والوحدات الجديدة التي تم انشاؤها في المرحلة الأولى، وكتب فوغارتي قائلاً: "بينما يكتسب قادة الجيش مجموعات وممثلين متزايدين يدمجون قدرات المعلومات في عمليات مستدامة، فإن" ARCYBER "، بالاشتراك مع قيادة التدريب والعقيدة وقيادة مستقبل الجيش "AFC"، سيكوف بمثابة جامع المعرفة الرئيسي للجيش من أجل القتال الحربي الناشئ في القرن الحادي والعشرين في بيئة المعلومات. وستنشئ" ARCYBER "مركزاً لعمليات حرب المعلومات في فورت جوردون وسيوفر المركز له ARCYBER قدرة غير مسبقة في الوقت الحقيقي لاستشعار وفهم بيئة المعلومات العالمية مع الاتصال بجميع أوامر مكونات خدمة الجيش.

وأضاف فوغارتي: ستسمح هذه الميزة الفريدة لذلك ARCYBER باستشعار وفهم واتخاذ القرار والاستجابة لظروف العنصر المعلوماتي العالمي الناشئ، مما

يوفر خيارات للقيادة العليا للجيش والقادة الإقليميين والجيش المشترك بسرعة لا مثيل لها، مما يتيح ميزة اتخاذ القرار الاستراتيجي.

ويهدف إنشاء هذا المركز إلى الاستفادة بشكل مباشر من دعم " ARCYBER " للقيادة السيرانية من خلال مقر القوة المشتركة وأوامر المقاتلين التي تدير العمليات السيرانية من أجلها، وسيكوف من الأمور الحاسمة لنجاح مركز العمليات التي توافر لواء استخبارات عسكري متخصص، وهو الذي سيركز فور تزويده بالموارد اللازمة، على بيئة المعلومات لتشمل الفضاء السيراني والطيف الكيرومغناطيسي.

ومع تطور حرب المعلومات، يمكن أن تتحول مهام الفرق الإلكترونية الهجومية التي ينفذها " ARCYBER " للقيادة الإلكترونية من خلال لواء الاستخبارات العسكرية 780 نحو تشكيل بيئة المعلومات .

وسيطور الجيش الأمريكي أيضاً قواته التكتيكية من خلال توسيع الأنشطة الإلكترونية والكيرومغناطيسية الحالية "CEMA"، داخل أقسام الأركان لتشمل علميات المعلومات والعمليات النفسية وموظفي الشؤون العامة وتعمل هذه الخلية على إعلام وتخطيط العمليات للقائد في القيادة داخل بيئة "CEMA"، وعلى نفس المنوال سيعمل الجيش على تحسين مكونات الاحتياط .

وأشار فوغارتي إلى أن العديد من القدرات المعلوماتية المتوافقة مع دعم القوات التقليدية تكمن في عناصر قوات الاحتياط، ووصف فوغارتي أيضاً قدراً لا بأس به من التجارب التي ستحدث في المرحلة الثانية مما سيساعد هذا على التطوير المستمر للقوات والقدرات لدعم العمليات متعددة المجالات. ستشمل هذه التجربة: (الاخضر، 2022)

أ. فرقة العمل متعددة المجالات، وتحديداً "ARCYBER"، وتساعد في تدريب واعداد كتيبة الاستخبارات والمعلومات والحرب الإلكترونية والحرب الإلكترونية والفضاء.

ب. قيادة معلومات مسرح العمليات، وهي مفهوم قيادة مستقبلية للجيش الأمريكي لقيادة من الرتب الشابة، تزود قادة مسرح العمليات بقدرات التأثير التي سيتم اختبارها خلال القتال الحربي المشترك وتدريبات الدفاع.

ت. ستجري فرقة عمل حرب المعلومات في أفغانستان، التي يقودها مجتمع العمليات الخاصة بالجيش الأمريكي، عمليات دعم المعلومات العسكرية وجمع وسائل التواصل الاجتماعي وتحليل البيانات وتكنولوجيا الإعلان الرقمي المتطورة لوسائل التأثير على الرأي العام.

المرحلة الثالثة:

ستبدأ المرحلة الثالثة اعتباراً من العام 2028 وما بعده، وستركز على القدرات متعددة المجالات، وأنه مهما كانت القيادة السيرانية للجيش الأمريكي، يجب أن تكون قادرة على النجاح في المعلومات والحرب غير التقليدية وأجراء عمليات استخباراتية واستطلاع مضاد للخصم وإظهار قدرة على الردع ذات مصداقية.

وأضاف فوغارتي كجزء من القوة المشتركة يجب أن يتقن الجيش إجراءات المنافسة الأساسية من خلال ما يسمى بعمليات متعددة المجالات "MDO"، ليصبح قادراً على تنفيذها في كل مهمة حاسمة. وستلعب "ARCYBER" دوراً داعماً أساسياً، حيث يطور الجيش بشكل أفضل قدرته على إجراء مشاركة نشطة من خلال

التوظيف المتقارب لقدرات المناورة والمعلومات التي تركز على تحقيق التأثيرات والسلوكيات المعرفية المرغوبة في خصوم الولايات المتحدة .

إنعكاسات الحروب السيبرانية على مستقبل الاستقرار الدولي

أدى اتساع علاقة الدول بالفضاء الإلكتروني، ومخافته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرحها على النحو الآتي: (لخضر، 2022)

1. تصاعد المخاطر الإلكترونية: خاصة مع قابلية المنشآت الحيوية ، مدنية وعسكرية في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو على أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يُعدّ أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب.

2. تعزيز القوة وانتشارها: فمن جهة، عزز الفضاء الإلكتروني القوة المؤسسية في السياسة الدولية وهي تعني أن يكوف لها دور في قوة الفاعلين، وتحقيق أهداف وقيم في ظل التنافس مع الآخرين والإسيما في تشكيل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية.

ومن جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تمثل ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولاً من غير الدول.

1. عسكرية الفضاء الإلكتروني، وذلك سعياً لدرء التهديدات على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

2. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة بيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

3. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حرباً للمستقبل، والتي يتم خوضها خوضاً بهدف تشتيت العدو، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق انظمتهم، واستخدام ونقل معلوماتهم وبياناتهم، وتزويد الدول الكبرى من يُحدد مصير تلك المعركة المُستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة، وضربها وتعطيلها.

4. تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية ورفع كفاءة الجاهزية القتالية لمثل هذه الحروب عن طريق التدريب، والمشاركة الدولية في حماية البنية

المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية. وهنا، يتعلق التوجيه الأخطر بنقل تمتلك □ القدرات من الدفاع إلى الهجوم عن طريق استخدام الهجمات في إطار إدارة الصراع بشكل دقيق وحساس في إطار إدارة الصراع والتوتر مع دول أخرى بشكل مُحترف.

تحول الحرب السيبرانية إلى حرب شاملة

مع استمرار تطور القدرات السيبرانية لعدد كبير من الفاعلين، سواء من الدول أو من الجماعات الإجرامية، وامتلاكهم للقدرة على التلاعب بالبنية التحتية الحيوية، فإن فرص تحول الحرب السيبرانية الاستراتيجية إلى حرب شاملة يظل قائماً. ويمكن تحديد الحالات التي يمكن فيها تحوّل الحرب السيبرانية إلى حرب شاملة: (عبدالوهاب، 2022)

1. استهداف البنية التحتية الحيوية: يلاحظ أن أحد الأمور التي سوف تحوّل المواجهات السيبرانية العدائية إلى حرب شاملة بين دولتين هو في حالة استهداف البنية التحتية الحيوية للدولة، وتسببها في خسائر فادحة، أو دمار كبير.

ومن الأمثلة على ذلك الهجمات على الشبكة الكهربائية التي تؤدي إلى انقطاع التيار الكهربائي بشكل كامل عن دولة معينة، أو الهجمات على المالي التي تؤدي إلى خسائر اقتصادية أو انهيار اقتصادي كامل، أو الهجمات على نظام النقل مما يؤدي إلى اصطدام الطائرات والقطارات، أو الهجمات على السدود التي تؤدي إلى فتح بوابات السدود، أو الهجمات ضد محطات الطاقة النووية، والتي تؤدي إلى انصهارها .

وعلى الرغم من أنه ليست هناك مؤشرات على حدوث مثل هذه النوعية من الهجمات بعد، فإن مثل هذا السيناريو قريب الحدوث. ففي ديسمبر 2014، أعلنت شركة كوريا الجنوبية للطاقة المائية والنوعية أن أنظمة الكمبيوتر لديها تعرضت لاختراق سيرياني، لكن لم تؤخذ منها سوى بيانات غير حساسة، غير أنه لم يعثر على أي فيروس ضار في وحدات التحكم بالمفاعلات، وهو ما يعني أن الهجوم لم يصل بعد إلى مرحلة التحكم في المفاعلات، أو التأثير على عملها، بصورة قد تتسبب في حدوث تسرب، أو انفجار نووي.

ولكن في حالة استمرار وتنامي الهجمات السيريانية، ونجاحها في التحكم في عمل المفاعلات، فإن مثل هذا التهديد سوف يفتح الباب أمام اندلاع حرب شاملة بين دولتين.

2. شن هجمات تقليدية وسيريانية متزامنة: يلاحظ أن مثل هذا السيناريو لا يعد مستبعداً، إذ إنه يتوقع في أي معارك مستقبلية أن تتم المزامنة بين شن الهجوم السيرياني والهجمات العسكرية التقليدية، وهو السيناريو الأسوأ الذي تستعد له أغلب الدول حول العالم.

3. تعطيل مرافق البنية التحتية الحيوية كافة: يقوم هذا السيناريو على قيام دولة أو عدة دول بشن هجمات سيريانية منسقة ومتزامنة تتسبب في انهيار الشبكة الكهربائية وفشل خطير في إمدادات الطاقة، مما يؤدي إلى توقف المستشفيات والقطارات والطائرات والنظام المالي عن العمل في غضون فترة زمنية قصيرة لا تزيد على خمس عشرة دقيقة، من دون أن يقوم إرهابي واحد أو جندي واحد بشن هجوم يستهدف هذا البلد".

ويلاحظ أن مثل هذا السيناريو يحتاج إلى قدرات سيرانية متطورة، بالإضافة إلى القدرة على مراقبة النظم الحيوية للخصم في مختلف القطاعات لشن هجمات متزامنة تستهدفها جميعاً في الوقت نفسه وهو أمر صعب الحدوث. ومع ذلك، فإن مثل هذا السيناريو سيكون تطبيقاً عملية لمقولة صن تزو المنظر العسكري الصيني، والذي أكد أن "تحقيق مائة انتصار في مائة معركة ليس أبصر ما يقوم به القائد، ولكن السيطرة على العدو من دون قتال هو الأبرع على الإطلاق".

الخاتمة

لمواجهة خطر الفضاء السيبراني لابد من أن يُطوّر استراتيجيته السيبرانية "Cyber Strategy" لفرض "توازن رعب جديد"، أو على أقل تقدير، خلق "توازن ردع نسبي، يستفيد إلى أقصى حد ممكن من هذا الفضاء السيبراني الواعد، ويؤدّي إلى كبح جماح من يحاول ان يفكر في اي اعتداء وعن اللجوء إلى شنّ " الحرب السيبرانية المفتوحة"، المقبلة حتمًا.

وعلينا أن نتذكّر أن التقدم المذهل في مجال الأسلحة التدميرية أفرز وضعًا دوليًا جديدًا يُعرف بإسم "توازن الرعب"، أو السلام بواسطة الردع، والنظام الدولي مُعرّض للتغيّر، وعوامل التغيّر كثيرة، يأتي التطوّر التكنولوجي في مقدّماتها، فالاختراعات في المجال العسكري كانت دائمًا العامل الأهم في تغيير مواقع الدول في سلّم القوى الدوليّة.

ومستوى التطوّر التكنولوجي في المجال العسكري سيُستخدم في المستقبل المنظور كمعيار لتحديد حجم القوّة العسكرية التي تملكها الدولة، ومن هذه الناحية فإنّ التمييز بين الدول لن يتمّ على أساس عديد أفراد الجيشبل على أساس مدى التقدم أو التخلف في تصنيع نوع جديد من الأسلحة التي من ضمنها برامج الحواسيب السّابحة في الفضاء السيبراني أو إنتاجه.

فالتكنولوجيا الحديثة استطاعت أن تُفرز عاملًا جديدًا في تغيير مواقع الدول في سلّم القوى الدوليّة، هو عامل الفضاء السيبراني الذي من شأنه قلب الآية والسماح لدولة مُزدهرة فيها صناعة برامج الحواسيب أو إنتاجها باحتلال مركز دولي مرموق

والتأثير في النظام الدولي من دون أن تكون مُتفوّقة عسكريًا بمعايير الدول الكبرى أو مَصافِها.

وصيانة الحياة والحرية والسيادة والاستقلال والمستقبل تُحتم علينا في المرحلة الراهنة أن نسعى جاهدين إلى تحويل المجتمع المُتخلف إلى مجتمع علمي، لأنّ التخلف، مدنيًا كان أم عسكريًا، لا يُمكن التغلّب عليه حتى ولو لم يكن هناك صراع مع اي عدو إلاّ بالثورة العلميّة الصادقة.

وأخيرًا، لا بدّ من الإقرار بأن موضوع أمن الفضاء السّيراني مشروع مُهم يستلزم إمكانيات ضخمة ولا يُمكن تنفيذه في مرحلة واحدة. وحتى لو توافرت الإمكانيات الماديّة والبشريّة اللازمة لإقامة هذا النظام الأمنيّ دفعة واحدة، فعلى أن نَعلم أنّ خباياه لم تتكشف كاملة بعد، فقد تُظهر تطبيقاته العمليّة عيوبًا تُحتم إعادة النظر فيه، وتَشذيبه، وبخاصّة وأنّه يعتمد على عنصر غير ثابت وسريع التطوّر وهو تكنولوجيا الإتصالات والمعلومات.

وأخيرًا لا بدّ من انتظار الوقت الكافي لترسيخ ما ظهر من مشاكل وحلول قانونيّة في حقل أمن الفضاء السّيراني وبلورة ما لم يُظهر حتى الآن، ونحن نتخيّل أنّ ما لم يُظهر كثير، نظرًا للتطوّر التقني المتسارع، ولكن لا يُمكن إزاء كل هذه التحدّيات أن نُبقي في القانون الدولي على نصوص خاصّة بالمرافق العامّة الدوليّة بعضها غير مُكتمل والبعض الآخر غير مُطبّق، تعود إلى زمانٍ غير زماننا السّيراني، لذلك يبدو من الضروري سنّ مُدونة سَيرانيّة مُتكاملة تحمي الفضاء السّيراني، وتُساعد على تعزيز مفهوم أمن الفضاء السّيراني.

المراجع والمصادر

المراجع العربية

<https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>.

1. الاوجلي، سالم محمد سليمان، (1997)، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، عين- شمس مصر.
2. إيفانز غراهام، نوينهام جيفري، (2004)، قاموس بنغوين للعلاقات الدولية، مركز الخليج للأبحاث. الإمارات العربية المتحدة: مركز الخليج للأبحاث .
3. ايهاب، خليفه: ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفلاتات الدولية؟ موقع المستقبل للأبحاث والدراسات المتقدمة، متاح على الرابط ، تاريخ الاطلاع : 2022-2-2-4: rku3jQ/ly.cutt//ht .
4. بارة سمي، (2017)، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، الجزائر.
5. بلقزيز، عبد الله، (1989)، الأمن القومي العربي، الهيئة المصرية العامة للكتاب، القاهرة- مصر.
6. بن داود، عبدالعزيز بن فهد، (2020)، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الأجهاد للدراسات القانونية والاقتصادية مجلد (9)، العدد 3، لسنة 2020.
7. بوغرة يوسف، (2018)، "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني". مجلة الدراسات الإفريقية وحوض النيل.

8. بونيف ، سامي محمد ، (2019) ، دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية، الردع السيبراني انموذجاً،المجلة الجزائرية للحقوق والعلوم السياسية، المجلد (4)، العدد (7) ، الجزائر .
9. التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الأصلح في الاتصالات للعام 2010-2011 .
10. التميمي، قاسم بلشان، (2021)، مفهوم الأمن السيبراني، معهد ابرار للدراسات، طهران - إيران .
11. جبور منى الأشقر، (2016)، السيبرانية هاجس العصر. بيروت: جامعة الدول العربية - المركز العربي للبحوث القانونية والقضائية.
12. الجهيني، منير محمد وممدوح محمد ،(2004)، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي، الاسكندرية-مصر.
13. حكيم ، غريب ، (2018) ، إلهاب السيبراني وألامن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية. المجلد 50، العدد 50، الجزائر .
14. خالد حسن أحمد لطفي ،(2020)، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي الطبعة الأولى، الاسكندرية -مصر .
15. خطاب، جمال، (2021) ، التهديدات السيبرانية آخذة في التطور. فلا تغفلوها، مجلة المجتمع ، تاريخ الاطلاع على الرابط: <https://mugtama.com/translations/item/132697-10.html>، 2022-1-20.
16. داود، عيسى سليم، (2017)، جرائم القرصنة الإلكترونية، رسالة ماجستير غير منشورة، جامعة الإسكندرية، الاسكندرية- مصر .

17. دحماني سليم، (2018)، "أثر التهديدات السيبرانية على الأمن القومي.. الولايات المتحدة الأمريكية أمودجاً، 2001-2017". جامعة محمد بوضياف المسيلة، قسم العلوم السياسية.
18. رغدة البهي، (2019)، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات". موقع المركز الديمقراطي العربي.
19. رمضان، مدحت، (2000)، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة-مصر.
20. الزرفي، علي نعمة جواد (2019)، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الاسكندرية مصر .
21. زروقة إسماعيل، (2019)، "الفضاء السيبراني والتحول في مفاهيم القوة والصراع". مجلة العلوم القانونية والسياسية، المجلد (10) العدد، (1) .
22. الزهراني، شيخه حسني، (2020)، التعاون الدولي في مواجهة الهجوم السيبراني كلية القانون، مجلة جامعة الشارقة، المجلد (14)، العدد (1) الشارقة- الامارات العربية المتحدة.
23. سعود، يحي ياسين، (2016)، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية.
24. السند، متعب بن عبدالله، (2011)، التعاون الدولي في تنفيذ الاحكام الجنائية واثره في تحقيق العدالة، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.

25. الشرقاوي، نسرين، (2021)، الإرهاب السيبراني وتداعياته النفسية والسياسية، المرصد المصري، القاهرة- مصر .
26. شكر، محمد، (2019)، الحرب السيبرانية وتداعياتها علي الأمن العالمي، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية.
27. الصحفي، روان بنت عطية الله ، (2020)، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرين، شهر 5.
28. طالة، لامية، (2020)، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد (40)، العدد (40).
29. الطيب مصطفى، (2019)، "الفرق بين أمن المعلومات والأمن السيبراني". مدونة علوم، 8 أغسطس.
30. عادل عبدالصادق، (2016)، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، المكتبة الأكاديمية، القاهرة-مصر.
31. عادل عبدالصادق، (2007)، هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي؟ ملف الأهرام الاستراتيجي، العدد 156 (ديسمبر 2007).
32. العازمي، فهد عبدالله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، القاهرة - مصر (2016).
33. العتيبي، عبد الرحمن بجاد شارع، (2017)، دور الأمن السيبراني في تعزيز الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية كلية العلوم الاستراتيجية، الرياض- السعودية .

34. عكاشه، أمير، (2012)، الحرب الإلكترونية صراع في العالم الافتراضي: الإنترنت في عالم اليوم أساس الاتصالات والتعاملات وأجهزة التحكم، ووسيلة للتجسس وأداة للحرب بمختلف صورها.
35. علي، نسرین الشحات، (2016)، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول "دراسة حالة إسرائيل"، المركز العربي الديمقراطي، برلين ألمانيا.
36. غانم، محمد حافظ (1962)، "المسؤولية الدولية"، معهد الدراسات العربية، القاهرة-مصر.
37. غيث، عالو، (2021)، الهجمات السيبرانية.. أكبر من حرب نووية بوسائل إلكترونية، موقع متخصص في الشؤون الإيرانية، بحث منشور على الإنترنت، تاريخه الاطلاع 2-2-2022، <https://jadehiran.com/archives/16835>.
38. الفتلاوي، احمد عيسى نعمة، (2016)، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد (4)، المجلد (8)، جامعة بابل، كلية القانون، بابل- العراق (2016) .
39. فلاك، نور الدين، (2012)، التهديدات السيبرانية عبر الفضاء الأزرق وتأثيرها على الأمن القومي للدول، الشعب أونلاين، تاريخ الاطلاع على الرابط : <http://www.ech-chaab.com/ar>، 20-1-2022.
40. القحطاني، مداوي سعيد، (2016)، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون الخليجي، مسابقة جائزة الامير نايف بن عبدالعزيز للبحوث الأمنية لعام (2015م)، الرياض-السعودية .

41. اللجنة الدولية للصليب الأحمر، (2019) القانون الدولي الإنساني والعمليات السيرية خلال النزاعات المسلحة، ورقة مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيرياني في سياق الأمن الدولي.

42. اللجنة الدولية للصليب الأحمر، (2019)، ورقة موقف: القانون الدولي الإنساني والعمليات السيرية خلال النزاعات المسلحة.

43. مجلس منظمة التعاون الاقتصادي والتنمية، (2015)، إدارة مخاطر الأمن الرقمي لتحقيق الزدهار الاقتصادي والاجتماعي: توصية 16 مجلس منظمة التعاون الاقتصادي والتنمية (OECD) والوثيقة المرفقة، نشر مجلس منظمة التعاون الاقتصادي والتنمية باريس،

<https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>.

44. مختار، محمد، (2015)، هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية؟ مفاهيم المستقبل مركز المستقبل للابحاث والتطوير، العدد 6.

45. مرزوق عنتر، حشاوي بن محيي الدين، (2017)، "الأمن السيرياني كبعد جديد في السياسة الدفاعية الجزائرية". ورقة بحث قدمت في الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقلة- الجزائر، 30- 31 يناير .

46. المعهد الوطني للمعايير والتقنية، (2017)، المنشور الخاص للمعهد الوطني للمعايير والتقنية) مسودة إطار عمل 13 إدارة المخاطر لانظمة المعلومات

والمنظمات: منهجية دورة حياة النظام للأمن والخصوصية، مسودة نقاش،

"سبتمبر 2017 [https://csrc.nist.gov/CSRC/media/Publications/](https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf)

[sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-](https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf)

[.draft.pdf](https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf)

47. مهمل، اسامه، (2018)، الإجرام السيبراني، رسالة ماجستير غير منشورة، كلية

الحقوق والعلوم السياسية جامعة محمد بوضياف، الجزائر.

48. يوسف حسن يوسف، (2011) الجرائم الدولية للإنترنت، المركز القومي

للإصدارات القانونية، القاهرة-مصر.

49. عبدالوهاب، شادي، (2022)، متى تتحول الحرب السيبرانية إلى حرب

شاملة؟ المستقبل للأبحاث والدراسات المتقدمة، القاهرة - مصر.

50. لخضر، بولطمين، (2022) الحرب السيبرانية : الخلفية، المستويات، والآثار

المستقبلية، مجلة أبحاث قانونية وسياسية المجلد 70، العدد (1)، الجزائر.

51. الحروب السيبرانية.. نتائج ملموسة لمعارك غير مرئية منشور على الرابط

<https://www.aljundi> بتاريخ 2021-4-1.

المراجع الأجنبية:

1. Australian Government, Attorney General's Department, National Plan to Combat Cybercrime, <http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf>.
2. Britain could carry out Cyber Attacks to defend itself against Russia, news, Telegraph, 2 February 2017.

3. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012): 188; See also, "Ralph Langner: Cracking Stuxnet, a 21 st Century Cyber Weapon", TED.
4. E. Nakashima. "U.S. Accelerating Cyberweapon Research", The Washington Post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html
5. Grant, Rebecca, (2007), "Victory in Cyberspace", The Eaker Institute, the policy and research arm, The Air Force Association of US, October 9, 2007.
6. Joseph S. Nye. *The Future of Power* (New York: Public Affairs, 2011).
7. KALAKUNTALA, Rohit, & others, (2019), *Cyber Security, HOLISTICA* Vol 10, Issue 2, 2019.
8. Myriam Dunn, "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", *Information and Security: An International Journal* 7 (2001): 145-158, online e-article, http://procon.bg/system/files/07.08_Dunn.pdf.
9. Olivier KEMPF, (2012), *Introduction à la Cyberstratégie*, Paris, Economica.
10. Robert McMillan, (2010), "Was Stuxnet Built to Attack Iran's Nuclear Program" *PC World*, http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.
11. Sommer, Peter & Brown, Ian (2011), "Reducing Systemic Cyber Security Risk", OCED.

